More Create Bloo

code16

CTFs Strona główna Mini arts Notes Magazine Found bugs

PIATEK, 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:

```
Types are poplished, excellent, man, platform, arrive, energy, denset, of
soft to Tipe, "Tipe-softing for properties," and by " or Effect for color
month, platform and control springs.
                                                                                          where to Total arrival bloomy office a service bloomy efficies a service bloomy enterting to page models blooming to the control of the contr
                                                                                                                                                                                               he ballade
a compleme
to the partied on a less thread
cortain sergus frances.
The package from EDDS (SMFMSE) M., 8 to 45000
```

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:

```
D_heiserbugs: Keep crashing testcases detected by hook, but when run via the debugger. buttonclicker: Spaam program to click buttons
rogram: Path to fuzzing target executable mdline_template: Used to specify the command-line invocation of
      pet:
program: c:\Program Files\IDA 6.6\idaq.exe
cmd inm.template: $PROGRAM = 0. -A. - - - SEEDFILE
cmd inm.template: $PROGRAM = 0. -A. - - - - C SEEDFILE
cmd inm.template: $PROGRAM = 0. -A. - - - C SEEDFILE
will result in the following invocation of Imagewagick:
# ci\rollowing invocation of Imagewagick
# ci\roll
```

TL;DR:

After a while we should be somewhere here:

```
0x17cc121f.0xe92422c7
0xb9a9edb4.0xc903f364 0x0b0cf415.0xc4ae2a21
0x69bf3fbe.0x6867f50e
0x69bf3fbe.0x8c329852
0x69bf3fbe.0xb9b46388
0x17cc121 131 folders selected (containing a total of 918 items).
```

O MNIE



code16 Cody Sixteen Wyświetl mój profil

ARCHIWUM BLOGA

- **2022** (16)
- **▶** 09 (1)
- **▶** 07 (3)

▼ 06 (1)

Night fuzzing session -IdaPro 6.6 - part 2

- **▶** 05 (1)
- **▶** 04 (7)
- **▶** 03 (1)
- **▶** 02 (2)
- **▶** 2021 (37)
- **▶** 2020 (62)
- **2019** (97)
- **2018** (67)
- **2017** (58)
- **2016** (63)

ETYKIETY

.net
android
binary
crackme
ctf
debug
docker
drones
enlil
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc

Case #81: ——CUID—— (1) (2) (3) (3) (3) (3) (3) (4) (4) (4		For example:
C-CI Minore Cital (1 Minore Debugo revor of 1 1001 100 200 200 200 200 200 200 200		
Commendation		Case #01:
Commendation		<cut></cut>
Maccost Macc	December	
Commondus for "Curringon Files (100 de cardina en en 1 di	Committation	
Expression protection control (1997) First control control (1997)	E-concide search point in: Medicand 0000000 0000000 000000 000000 0000000 0000	Copyright (c) Microsoft Corporation. All rights reserved.
Cont. Cont	Execution continues of the continue of the con	CommandLine: "C:\Program Files\IDA 6.6\idaq.exe" -B -A -ac C:\FOE2\fuzzdir\campaign_ijatnp\iteration_m_yrvq\foe-crash-I0mnvu\sf_0d75862d5d90166274cc61a363c74828-576.exe
Column C	Medical 0000000 000000000 Majorani	
[Column C	
	Clab Clab Access within - cando (Collos) (et al transic)	
The second control con	This controlloops are presented and mandance. ***Controlloops are controlloops are control	
	######################################	First chance exceptions are reported before any exception handling.
	Carticological controlled contr	This exception may be expected and handled.
carbotis acetions decoded acetions aceticated acetions acetions acetions acetions acetions acetions acetions aceticated acetions	Control Cont	
######################################	######################################	
77559966 Bc448de mov accident pit (ein-ear'4-4) doc0203095000000000000000000000000000000000	### ### ### ### ### ### ### ### ### ##	
0.000 r;rilespication evultor;r emonitorionose emonitorionos emonitorios	Control	
		The second of the second secon
sp=77559886 sp=008botk dep=008botk logi=0		0:000> r,r;lexploitable -v;kb;r;q
Seriol 10 Seriol 20 Seri	car-001s car-0023 dar-0023 dar-00203 fa-00000 qui-00000 qui-000000 qui-0000000 qui-0000000 qui-00000000 qui-0000000 qui-0000000 qui-00000000 qui-00000000 qui-0000000 qui-00000000 qui-00000000 qui-00000000000 qui-000000000 qui-00000000000 qui-000000000000000 qui-000000000000000000000000000000000000	eax=00000000 ebx=07de0ba8 ecx=00000007 edx=00000000 esi=02532fe8 edi=005bc114
######################################	######################################	
7559968 Ba48ec	77599688 804-804c	
eau-00000000 etu-07 de/tibale ecu-00000007 edu-000000000 esi-000524 fee dei-0050ct 14 elei-profitosibel de jef-0050ct foi pie o no vue el ny no a pe y control se en control se en colo se	eau-footcools also-off-acidate acid-occools period on to up in part acid part of acid to acid period	
elga-775509806 esg-0036cbdil ebg-0036cbdil togla of in var pe in graz ac pe cy ca-001 to sa-0023 di-00323 oi-00323 oi-0038 gi-0030 oi-00397 movertimemapy-n0.dei. **Top569806 8bd-64e** or or ext., dword pit [esi+ecx*4-1] dis 0023 02533000+77777777 **Leapfollable 1.6.0 **Leapfollable	eign=775500066 eag=002064cd(a stop=003054cd005 (spin0) in vivu pi nig na acipe ny ce-n011s sero0203 fe-n0035 ge-n0030 ge-n001000 eign-00010297 monvertimenergy-th-056: 77550066 8b4-64 in mov eax.dword ptr (sein-ecx*4-ij dis 0023 0253000-77777777	
Case Color Case Color Case Color Case	ca-001b sen0023 de-0023 en0028 pen0028 pen003 gen000 enteronograph resortmerceptrub.66. 775596968 bladdelic mov eax,dword pir [esi+ecx'4-4] de-0023.0253000-77777777 Respitable 15.0.0 Respitable 15.0.0	
r7559960 80448efc nov eax.dword ptr [esi+ecx*4.4] ds:0023:02533000-r77777777 lesploitable 1.6.0.0 HostMachinelHostUser Executing Processor Architecture is x86 Debuggee is in User Mode Debuggee is in User Mode Exception Faulting Address: 0:2533000 First Chaine Exception Type: STATUS ACCESS_VIOLATION (0x.0000005) Exception Sub-Type: Read Access Violation Faulting Instruction:77559966 mov eax.dword ptr [esi+ecx*4.4] Tainted Input operands: 'ecx', 'esi' 77559968 mov dword ptr [esi+ecx*4.4] eax Tainted Input operands: 'ecx', 'esi' 77559968 mov dword ptr [esi+ecx*4.4] eax Tainted Input operands: 'ecx', 'esi' 77559975 add esi, eax Tainted Input operands: 'ecx' 77559975 add esi, eax Tainted Input operands: 'ecx' 77559975 add esi, eax Tainted Input operands: 'ecx' 77559977 pro dword ptr msvertmemorpy+0x88 (77559968)(edx'4) Exception Hash (Miglor/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Replace Repl	
texploitable 1.8.0.0 HostMachine/HostUser Executing Processor Architecture is x88 Debuggee is in User Mode Debuggee is in User Mode Debuggee is in User Mode Event Type: Exception Event Type: Exception Event Type: Exception Faulting Address: 0x2533000 First Chance Exception Type: STATUS_ACCESS_VOLATION (0xC0000005) Exception Sub-Type: Read Access Volation Faulting Instruction:77559988 mov eax.dword ptr [esi+ecx*4-4] Basic Block: 77559986 mov eax.dword ptr [esi+ecx*4-4] Tainted typut operands: 'eox', 'ear' 77559986 mov dword ptr [edi+ecx*4-4], aax Tainted typut operands: 'eax', 'eox' 77559987 add eai.eax Tainted typut operands: 'eax', 'eox' 77559987 add eai.eax Tainted typut operands: 'eax', 'ear' 77559987 add eai.eax Tainted typut operands: 'eax', 'ear' 77559997 add eai.eax Tainted typut operands: 'eax', 'ear' 77559997 add eai.eax Tainted typut operands: 'eax', 'ear' 77559997 ping dword ptr msverttmemcpy+0xa8 (7755998)[edx*4] Exception Hash (MajortMinor): 0x17cc1211.0x62867b4b	Hespitalate I is 0.0 Hespitalate I is 0.0 Debugges is in User Mode Exception Faulting Address: 0x2533000 First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005) Exception Sub-Type: Read Access Violation Faulting Instruction:773569866 mov eax.dword ptr [esi+ecx*4-4] Basic Block: 775599866 mov eax.dword ptr [esi+ecx*4-4] Tained input operands: "eax", eax' 775599876 lea eax.[eax"4] Tained input operands: "eax", eax' 775599877 add ed. eax Tained input operands: "eax", eax' 77559977 add ed. eax Tained input operands: "eax", eax' 77559977 add ed. eax Tained input operands: "eax", eax' 77559977 abd ed. eax Tained input operands: "eax", eax' 77559977 abd ed. eax Tained input operands: "eax", eax' 77559977 jump dword ptr mavortimemopy+0xa8 (775598b5)[edx*4] Exception Habi (MajortMinor): 0x17c1211.0x1286754b Habi Usage: Stack-Trace: Major+Minor: mavortimemopy+0x56 Major+Minor: avgortimeTemopy+0x66 Major+Minor: doghelptSymGetModuleInfoW64+0x549	msvcrtlmemcpy+0x56:
Hash Machinel Host User Executing Processor Architecture is x86 Debuggee is all we 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: 77559988 mov eax_dword ptr [esi+ecx*4-4] Basic Block: 77559986 mov eax_dword ptr [esi+ecx*4-4] Tainted input operands: 'ecx', 'esc' 77559986 mov dword ptr [edi+ecx*4-4] eax Tainted input operands: 'ecx', 'ecx' 775599875 and esi.eax Tainted input operands: 'ecx', 'ecx' 775599875 and esi.eax Tainted input operands: 'ecx', 'ecx' 77559987 and esi.eax Tainted input operands: 'ecx', 'esc' Trainted input operands: 'ecx',	Executing Processor Architecture is x86 Debuggee is a live war mode debugging session on the local machine Event Type: Exception Exception Faulting Address: 0x2533000 First Chance Exception Type: STATUS_ACCESS_VIOLATION (0x0000005) Exception Sub-Type: Read Access Violation Faulting Instruction:77559966 mov eax, dword ptr [esi+exc*4-4] Basic Block: 77559968 mov eax, dword ptr [esi+exc*4-4] Tainted input operands: 'eax', 'esi' 77559968 mov dword ptr [edi-exc*4-4].eax Tainted input operands: 'eax', 'esc' 77559968 mov dword ptr [esi-exc*4-1] Tainted input operands: 'eax', 'esc' 77559968 mov dword ptr [esi-exc*4-1] Tainted input operands: 'eax', 'esc' 77559967 and esi-eax; [exc*4] Tainted input operands: 'eax', 'esc' 77559977 and esi-eax; [exc*4] Tainted input operands: 'eax', 'esc' 77559978 pro dword ptr promote 'eax', 'esc' 77559978 pro dword ptr promote 'eax', 'esc' 77559979 pro dword ptr promote 'eax', 'esc' 77559979 pro dword ptr promote 'eax', 'esc' 77559979 pro dword ptr mworttmemcpy+0xx8 (7755998)[edx*4] Exception Hash (Major/Minor): 0x17cs121f.0x0286724b Major-Minor: -mworttmemcpy+0x56 Major-Minor: -dbyheip(SymCeMhoduleinfoW84+0x54b)	77559966 8b448efc mov eax,dword ptr [esi+ecx*4-4] ds:0023:02533000=????????
Exception Faulting Instruction: 77559986 mov eax.dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx' esi 77559986 is a lex (xe') esi 77559986 is a lex (xe') esi 77559986 is a lex (xe') esi 77559986 mov eax.dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx' esi 77559986 mov eax.dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx' esi 77559986 mov eax.dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx' esi 77559986 mov eax.dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx' esi 77559987 and esi, eax Tainted Input operands: 'ecx' 7755997 and edi, eax Tainted Input operands: 'ecx' 7755997 and edi, eax Tainted Input operands: 'ecx' esi 7755997 and edi, eax Tainted Input operands: 'ecx' esi 7755997 and edi, eax Tainted Input operands: 'ecx' esi 7755997 and edi, eax Tainted Input operands: 'eax' esi 77559970 and edi, eax Tainted Input operands: 'eax' esi 77559970 and edi	Executing Processor Architecture is x86 Debuggee is in User Mode Debuggee is in User Mode Debuggee is in User Mode Exception Faulting Address: 0x2533000 First Channel 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: 77555968 mov eax.dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx', 'esi' 77555968 mov dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx', 'esi' Trissoffs and esi-eax Tainted Input operands: 'ecx', 'esi' Trissoffs and esi-eax, 'ecx' Trissoffs and esi-eax Tainted Input operands: 'ecx', 'esi' Trissoffs and esi-eax Tainted Input operands: 'eax', 'esi' Trissoffs and esi-eax Tainted Input operands: 'eax' esi' Trissoffs and esi-eax esi' Trissoffs and esi-eax esi' Trissoffs and esi-eax esi' Tr	!exploitable 1.6.0.0
Debuggee is in User Mode Debuggee is a live user mode debugging session on the local machine Event Type: Exception Exception Fauting 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: 'eex', 'esi' 77559968 mov dword ptr [edi-ecx*4-4].eax Tainted Input operands: 'eax', 'ecx' 77559966 lea eax,[eox*4] Tainted Input operands: 'eax', 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax', 'esi' 77559979 jmp dword ptr msvorttmemcpy+0xa8 (7755998b)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Debuggee is a live user mode debugging session on the local machine Event Type: Exception Event Type: Exception 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: 77559986 mov eax.dword ptr [esi+ecx*4-4] Tained Input operands: 'ecx', 'esr' 77559986 mov dexx ptr [esi+ecx*4-4] eax Tainted Input operands: 'ecx', 'esr' 77559975 add esi, eax Tainted Input operands: 'ecx', 'esr' 77559977 add edi, eax Tainted Input operands: 'eax', 'esr' 77559977 add edi, eax Tainted Input operands: 'eax', 'esr' 77559979 jmp dword ptr mevertimencpy+0x86 (77559988)[edx*4] Exception Hash (Major/Minor: Ox17cc121f.0x62867b4b Major+Minor: insvertimencpy+0x56 Major+Minor: dbyhelp/Stack/win644+0x1bba Major+Minor: dbyhelp/Stack/win644+0x1bba	HostMachine\HostUser
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:77599966 mov eax,dword ptr [esi+ecx*4-4] Basic Block: 77559966 mov eax,dword ptr [esi+ecx*4-4] Tainted Input operands: 'eax', 'ear' 77559968 mov dword ptr [edi+ecx*4-4].eax Tainted Input operands: 'eax', 'ear' 775599696 lea eax_(ecx*4] Tainted Input operands: 'eax', 'ear' Tossee? Tainted Inp	Debuggee is a live user mode debugging session on the local machine Event Typne Exception Exception Faulting Address: 0x2533000 First Chance Exception Types: 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] Tained Input operands: eox*,	Executing Processor Architecture is x86
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: 'eax', 'esi' 77559968 mov dword ptr [edi+ecx*4-4] eax Tainted Input operands: 'eax', 'ecx' 77559968 mov dword ptr [edi+ecx*4-4] eax Tainted Input operands: 'eax', 'ecx' 77559975 add esi, eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax', 'esi' 77559979 jmp dword ptr moverthemcpy+0xa8 (77559988)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b	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" 77559968 mov dword ptr [esi+ecx*4-4] eax Tainted Input operands: "ecx*,esi" 77559968 eis eax,[ecx*4] Tainted Input operands: "ecx*,esi" 77559969 eis eax,[ecx*4] Tainted Input operands: "ecx*,esi" 77559973 add esi,eax Tainted Input operands: "eax*,esi" 77559979 pm dword pr mavertimencpy+0xa8 (77559988)[edx*4] Exception Hash (Major/Minor): 0x17cs121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: dbghelp/Stack/Walk64+0x1bba Major+Minor: dbghelp/Stack/Walk64+0x1bba	
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," esr" 77559969 mov dword ptr [edi+ecx*4-4].eax Tainted Input operands: "eax," ecx Trible Input operands: "eax," ecx Trible Input operands: "eax," ecx Trible Input operands: "eax," exc Trible Input operand	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: 77559968 mov eax,dword ptr [esi+ecx*4-4] Tainted Input operands: 'ecx', 'esi' 77559968 mov don'd ptr [edi+ecx*4-4] Tainted Input operands: 'ecx', 'esi' 77559968 eax [ecx*4] Tainted Input operands: 'ecx', 'ecx' 77559975 and esi, eax Tainted Input operands: 'eax', 'ecx' 77559977 and edi, eax Tainted Input operands: 'eax', 'esi' 77559977 and edi, eax Tainted Input operands: 'eax' esi' Tainted Input operands: 'eax' esi' Tainted Input operands: 'eax' esi' Tainted Input operands: 'eax' First (sign) (sign) Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: dbyhelp/StackWallk64+0x1bba Major+Minor: dbyhelp/StackWallk64+0x1bba	
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' 77559968 mov dword ptr [esi+ecx'4-4], eax Tainted Input operands: 'eax', 'ecx' 77559969 lea eax,[ecx'4] Tainted Input operands: 'eax', 'esx' 77559975 add esi,eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax' Tossp977 add edi,eax Tainted Input operands: 'eax' Tainted Input operands: 'eax' Tossp979 jmp dword ptr msvertlmemcpy+0x88 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62887b4b	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' 77559968 mov dword ptr [edi+ecx*4-4].eax Tainted Input operands: 'eax', 'ecx' 77559975 add esi, eax Tainted Input operands: 'eax', 'esi' 77559977 add edi, eax Tainted Input operands: 'eax', 'esi' 77559979 jimp dword ptr mexcrttmencpy+0xa8 (77559988)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: dbyhelp/StackWall&64+0x1bba Major+Minor: dbyhelp/StackWall&64+0x1bba	
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' 7755996e nov 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 msvcrtlmemcpy+0xa8 (77559988)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Faulting Instruction:77559986 mov eax,dword ptr [esi+ecx'4-4] Basic Block: 77559966 mov eax,dword ptr [esi+ecx'4-4] Tainted input operands: 'ecx', 'esr' 77559986 mov dword ptr [eti+ecx'4-4],eax Tainted input operands: 'eax', 'ecx' 7755998e lea eax,[ecx'4] Tainted input operands: 'eax', 'ecx' 77559975 add esi,eax Tainted input operands: 'eax', 'esr' 77559975 add esi,eax Tainted input operands: 'eax', 'esr' 77559978 add esi,eax Tainted input operands: 'eax', 'esr' 77559979 jmp dword ptr msvcrttmemcpy+0x88 (77559988)[edx'4] Exception Hash (Major/Minor): 0x17cs121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvcrttmemcpy+0x56 Major+Minor: dbghelp/StackWalk64+0x1bba Major+Minor: dbghelp/SymGetModuleInfoW64+0x549	
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', 'esi' 77559979 jmp dword ptr msvortImemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b	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: 'eax', 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax', 'esi' 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	
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', 'esi' 77559979 jmp dword ptr msvortImemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b	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: 'eax', 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax', 'esi' 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	Faulties Industrial 77550000 was any droug at faci and 41
Trinted Input operands: 'ecx', 'est' Trispage mov dword ptr [edi+ecx'4-4],eax Tainted Input operands: 'eax',ecx' Trispage lea eax, [ecx'4] Tainted Input operands: 'ecx' Trispage lea eax, [ecx'4] Tainted Input operands: 'ecx' Trispage lea eax, [ex'4] Tainted Input operands: 'eax' Tainted Input operands: 'eax',esi' Trispage raid edi,eax Tainted Input operands: 'eax' Tainted Input operands: 'eax' Trispage raid edi,eax Tainted Input operands: 'eax' Trispage raid edi,eax Tainted Input operands: 'eax' Trispage raid edi,eax Trispage r	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: 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax' 77559977 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvorttmemcpy+0xa8 (775599b8)(edx*4) Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvorttmemcpy+0x56 Major+Minor: dbghelplStack/Walk64+0x1bba Major+Minor: dbghelplSymGetModuleInfoW64+0x549	, daming manadona oddou mur can,arona pa [bar can नन]
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' Tainted Input operands: 'eax' Tainted Input operands: 'eax' Teinted Input operands: 'eax' Teinted Input operands: 'eax' Tainted Input operan	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: 'eax' 77559975 add esi,eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax', 'esi' 77559979 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvertlmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvertlmemcpy+0x56 Major+Minor: dbghelp StackWalk64+0x1bba Major+Minor: dbghelp StackWalk64+0x1bba	Basic Block:
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' Tainted Input operands: 'eax' Text operands: 'eax' Tainted Input operands: 'eax' Text operands: 'eax' Tiented Input operands:	Trainted Input operands: 'eax', 'ecx' Trainted Input operands: 'eax', 'ecx' Trainted Input operands: 'eax', 'ecx' Trainted Input operands: 'eax' Trainted Input operands: 'eax' Trainted Input operands: 'eax', 'esi' Trainted Input operands: 'eax', 'esi' Trainted Input operands: 'eax' Trainted Input operands: 'e	
Tainted Input operands: 'eax', 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax', 'esi' 77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Tainted Input operands: 'eax', 'ecx' 7755996e lae aex.[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 msvcrttmemcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvcrttmemcpy+0x56 Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplStymGetModuleInfoW64+0x549	
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' Tainted Input operands: 'eax' Trinted Input operands: 'eax' 77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	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 msvcrttmemcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvcrttmemcpy+0x56 Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplStymGetModuleInfoW64+0x549	
Tainted Input operands: 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax','esi' 77559979 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Tainted Input operands: 'ecx' 77559975 add esi,eax Tainted Input operands: 'eax','esi' 77559977 add edi,eax Tainted Input operands: 'eax' Tainted Input operands: 'eax' 77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvcrttmemcpy+0x56 Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplStymGetModuleInfoW64+0x549	
Tainted Input operands: 'eax','esr' 77559977 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvort!memcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Tainted Input operands: 'eax', 'esi' 77559977 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvorttmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvorttmemcpy+0x56 Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplSymGetModuleInfoW64+0x549	
77559977 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	77559977 add edi,eax Tainted Input operands: 'eax' 77559979 jmp dword ptr msvort!memcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvort!memcpy+0x56 Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplStymGetModuleInfoW64+0x549	77559975 add esi,eax
Tainted Input operands: 'eax' 77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx'4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	Tainted Input operands: 'eax' 77559979 jmp dword ptr msvorttmemcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace: Major+Minor: msvorttmemcpy+0x56 Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplSymGetModuleInfoW64+0x549	Tainted Input operands: 'eax','esi'
77559979 jmp dword ptr msvcrtfmemcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage: Stack Trace:	77559979 jmp dword ptr msvcrttmemcpy+0xa8 (775599b8)[edx*4] Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage : Stack Trace: Major+Minor : msvcrttmemcpy+0x56 Major+Minor : dbghelplStackWalk64+0x1bba Major+Minor : dbghelplSymGetModuleInfoW64+0x549	77559977 add edi,eax
Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage : Stack Trace:	Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b Hash Usage : Stack Trace: Major+Minor : msvcrttmemcpy+0x56 Major+Minor : dbghelplStackWalk64+0x1bba Major+Minor : dbghelplSymGetModuleInfoW64+0x549	
Hash Usage: Stack Trace:	Hash Usage: Stack Trace: Major+Minor: msvcrt/memcpy+0x56 Major+Minor: dbghelp/StackWalk64+0x1bba Major+Minor: dbghelp/SymGetModuleInfoW64+0x549	торяятя Jmp awara ptr msvartimemcpy+uxas (торяява)[eax-4]
	Major+Minor : msvort!memcpy+0x56 Major+Minor : dbghelplStackWalk64+0x1bba Major+Minor : dbghelplSymGetModuleInfoW64+0x549	Exception Hash (Major/Minor): 0x17cc121f.0x62867b4b
Mojora-Minor - mojort/momonya-0v56	Major+Minor: dbghelplStackWalk64+0x1bba Major+Minor: dbghelplSymGetModuleInfoW64+0x549	Hash Usage : Stack Trace:
	Major+Minor : dbghelplSymGetModuleInfoW64+0x549	
	Water Transport Control of Technology (Control of Technology Control of Technology Contr	Major+Minor : dbghelplSymGetModuleInfoW64+0x549 Major+Minor : dbghelplFindExecutableImage+0x80e

Major+Minor : dbghelp!StackWalk64+0x2a85

pwn RE web writeup

```
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
      : SYSFER+0x45b1b
Minor
      : SYSFER+0x45b1b
Minor
      : SYSFER+0x45a1c
Minor
Minor
      : idaq+0x70000
      : idaq+0x70000
Minor
      : idaq+0x70000
Minor
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+0x000000000000066 (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 idag+0x70000
005bd0b8 00100000 00001000 00000000 00000010 idag+0x70000
005bd174 726aa175 66bff840 000000e8 031597c0 idag+0x70000
eax=00000000 ebx=07de0ba8 ecx=00000007 edx=00000000 esi=02532fe8 edi=005bc114
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000
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.
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
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
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010297
msvcrt!malloc+0xcf:
lexploitable 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!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 : dba+0x9f2f
Minor : SYSFER+0x45b1b
Minor : SYSFER+0x45b1b
Minor : SYSFER+0x45a1c
Instruction Address: 0x000000077559dbd
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+0x000000000000000cf called from
dbghelp!StackWalk64+0x000000000001bba (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 msvcrtlmalloc+0xcf

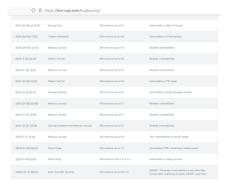
```
0025bb50 679a1059 08250ba8 00000000 06790000 dbghelp!StackWalk64+0x1bba
0025befc 679c8036 08250ba8 00000002 00000000 dbghelp!SymGetModuleInfoW64+0x549
0025bf14 679a6a2c 08250ba8 4794d435 00000000 dbghelp!FindExecutableImage+0x80e
0025c3a4 679a6ca6 beeffeed 0824b518 00400000 dbghelp!StackWalk64+0x2a85
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 fffffffe dbg+0x9f2f
0025cc4c 753d5b1b fffffffe 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
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000
msvcrt!malloc+0xcf:
---<cut>---
Another variant below.
Case #03:
---<cut>---
(...)
Microsoft (R) Windows Debugger Version 6.11.0001.404 X86
Copyright (c) Microsoft Corporation. All rights reserved.
Command Line: "C: Program Files IDA 6.6 idaq.exe" - B - A - a - c C: FOE2 fuzz diric ampaign\_egm\_o8 literation\_l frill foe-crash-oxqtdmisf\_76 ffd62 at f8250 f56 b56 d8a a211b31a9-252 for files IDA for files IDA
(...)
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
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000
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!memcpv+0x57:
68ee1ed7 f3a5
                         rep movs dword ptr es:[edi].dword ptr [esi]
eax=03b8bba0 ebx=0a00001c ecx=02800007 edx=00000000 esi=f9b8bb84 edi=086a0020
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
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 Exploitability Classification: PROBABLY_EXPLOITABLE 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 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)

Motyw Okno obrazu. Obsługiwane przez usługę Blogger.