TREE Case Study - BasicOVPlus.exe

Basic Overflow Plus

Vulnerability Name: Basic Overflow Plus Example
Application Mode: User Mode
Target: Windows

Sample ran on:
Windows 7 32-bit for IDA 6.4 environment

Description

Basic buffer overflow. The overflow occurs when the input file "mytaint.txt" has more than 8 bytes.

BasicOVPlus.cpp

```
// filebufov.cpp : Defines the entry point for the console application.
//

#include "windows.h"
#include <stdio.h>

HANDLE hFile = NULL;

void StackOVflow(char * sBig,int num);

int main(int argc, char* argv[])
{
 char sBigBuf[16]={0};

 hFile = CreateFile("mytaint.txt",      // Open One.txt
       GENERIC_READ,           // Open for reading
       0,                      // Do not share
       NULL,                   // No security
       OPEN_EXISTING,          // Existing file only
       FILE_ATTRIBUTE_NORMAL,  // Normal file
       NULL);                  // No template file

 if (hFile == INVALID_HANDLE_VALUE)
 {
  return 1;
 }

 DWORD dwBytesRead;
 ReadFile(hFile, sBigBuf, 16, &dwBytesRead, NULL);

 CloseHandle(hFile);

 for(int i=0; i< (dwBytesRead-2); i++)
  sBigBuf[i] +=sBigBuf[i+1];

 StackOVflow(sBigBuf,dwBytesRead);

 return 0;
}
```

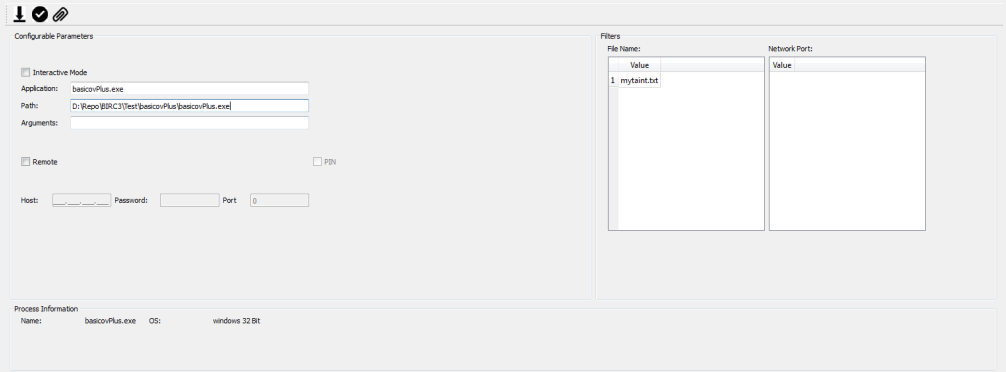
```
void StackOVflow(char *sBig,int num)
{
 char sBuf[8]= {0};

 for(int i=0;i<num;i++)
 {
  sBuf[i] = sBig[i];
 }
 return;
}


void Hack()
{
 MessageBox(NULL,"CBASS(Cross-platform Binary Automated Symbolic-execution
System) \n               Hacking Demo ","*** You Have Been Owned!!!
```

```
***",0x00001010);
 exit(-1);
}
```

Configuring the Tracer

Indicate mytaint.txt file content for the overflow.

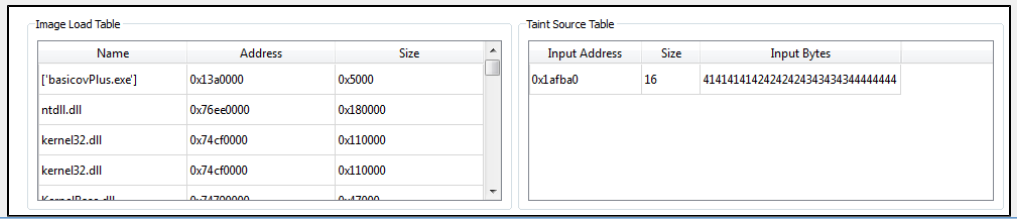
Configuring the Tracer



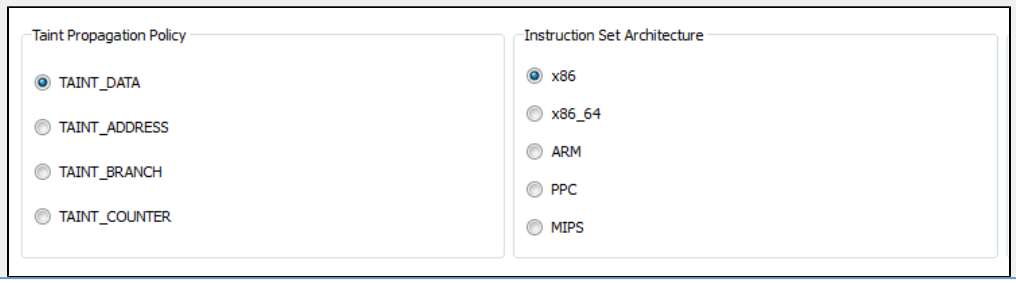
Application: basicovPlus.exe
Path: ...\basicovPlus.exe

Filters: mytaint.txt

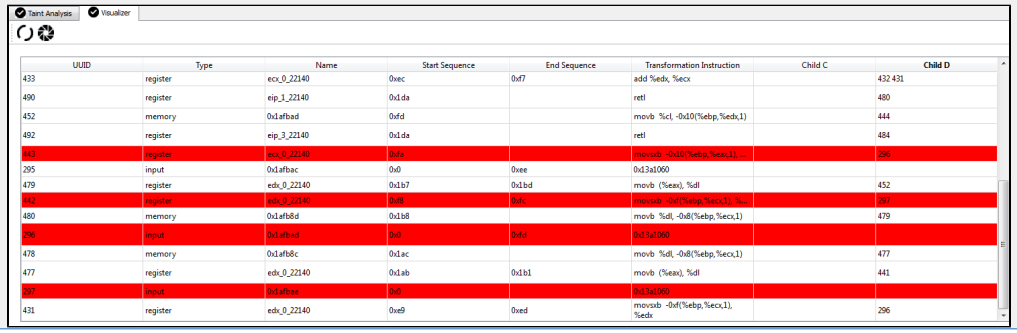
Taint Propagation Policy - Taint Data



Taint Data



Taint Table



Taint Analysis | Visualizer

UUID	Type	Name	Start Sequence	End Sequence	Transformation Instruction	Child C	Child D
433	register	ecx_0_22140	0xec	0xf7	add %edx, %ecx		432 431
490	register	eip_1_22140	0x1da		retl		480
452	memory	0x1afbad	0xfd		movb %cl, -0x10(%ebp,%edx,1)		444
492	register	eip_3_22140	0x1da		retl		484
443	register	ecx_0_22140	0xfa		movsxb -0x10(%ebp,%eax,1), ...		296
295	input	0x1afbac	0x0	0xee	0x13a1060		
479	register	edx_0_22140	0x1b7	0x1bd	movb (%eax), %dl		452
442	register	edx_0_22140	0xf8	0xfc	movsxb -0xf(%ebp,%ecx,1), %...		297
480	memory	0x1afb8d	0x1b8		movb %dl, -0x8(%ebp,%ecx,1)		479
296	input	0x1afbad	0x0	0xfd	0x13a1060		
478	memory	0x1afb8c	0x1ac		movb %dl, -0x8(%ebp,%ecx,1)		477
477	register	edx_0_22140	0x1ab	0x1b1	movb (%eax), %dl		441
297	input	0x1afbae	0x0		0x13a1060		
431	register	edx_0_22140	0xe9	0xed	movsxb -0xf(%ebp,%ecx,1), %edx		296

Taint Graph