

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 StackOverflow(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];

    StackOverflow(sBigBuf,dwBytesRead);

    return 0;
}
```

```
void StackOverflow(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

The screenshot shows the 'Configurable Parameters' window of a tracer. The 'Interactive Mode' section is active, with the following settings:

- ☒ Interactive Mode
- Application: basicovPlus.exe
- Path: C:\Program Files\test\basicovPlus\basicovPlus.exe
- Arguments: (empty)
- ☐ Remote
- ☐ PDV
- Host: (empty)
- Password: (empty)
- Port: 0

The 'Filters' section on the right shows a table with one entry:

File Name:	Value
1 mytaint.txt	

The 'Process Information' section at the bottom shows:

Name: basicovPlus.exe OS: windows 32 Bit

Application: basicovPlus.exe

Path: ...\\basicovPlus.exe

Filters: mytaint.txt

Taint Propagation Policy - Taint Data

Image Load Table			Taint Source Table		
Name	Address	Size	Input Address	Size	Input Bytes
['basicovPlus.exe']	0x13a0000	0x5000	0x1afba0	16	414141414242424243434344444444
ntdll.dll	0x76ee0000	0x180000			
kernel32.dll	0x74cf0000	0x110000			
kernel32.dll	0x74cf0000	0x110000			
kernel32.dll	0x74cf0000	0x110000			

Taint Data

Taint Propagation Policy

- ☒ Taint_DATA
- ☐ Taint_ADDRESS
- ☐ Taint_BRANCH
- ☐ Taint_COUNTER

Instruction Set Architecture

- ☒ x86
- ☐ x86_64
- ☐ ARM
- ☐ PPC
- ☐ MIPS

Taint Table

UUID	Type	Name	Start Sequence	End Sequence	Transformation Instruction	Child C	Child D
433	register	ecx_0_22140	0xac	0xf7	add %edx, %ecx	432	431
490	register	eip_1_22140	0x1da		retl		480
452	memory	0x1afbad	0xf0		movb %cl, 0x10(%ebp, %edx, 1)		444
492	register	eip_3_22140	0x1da		retl		484
453	register	eax_0_22140	0xf4		movsbl 0x10(%ebp, %edx, 1) %eax		250
295	input	0x1afbdc	0x0	0xee	0x13a1000		
479	register	edx_0_22140	0x1b7	0x1bd	movb (%eax), %dl		452
451	register	eax_0_22140	0xf8	0xf9	movsbl 0x10(%ebp, %edx, 1) %eax		297
480	memory	0x1afb8d	0x1b8		movb %dl, 0x1(%ebp, %ecx, 1)		479
296	input	0x1afb8d	0xf0	0xf4	0x13a1000		
478	memory	0x1afb8c	0x1ac		movb %dl, 0x1(%ebp, %ecx, 1)		477
477	register	edx_0_22140	0x1ab	0x1b1	movb (%eax), %dl		441
297	input	0x1afb8e	0xf0		0x13a1000		
431	register	edx_0_22140	0x0b	0x0d	movsbl 0x1(%ebp, %ecx, 1) %edx		296

Taint Graph

