

[VulnWatch] 5 bugs

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0025.html>

From: D4rkGr3y (grey_1999@mail.ru)

Date: 07/12/02

Date: Fri, 12 Jul 2002 22:35:31 +0400

From: D4rkGr3y <grey_1999@mail.ru>

To: bugtraq@securityfocus.com, vulnwatch@vulnwatch.org

Hi

I want to advice about some bugs that founded by our team (DHGroup :: www.dhgroup.org):

1. Eserv/2.97 (www.eserv.ru)

This is shareware `http/ftp/pop/smtp/proxy` server.

Directory travel vuln was founded in `http-server`.

Exploit:

`www.somehost.com/somedir/?`

This url will show content of directory "somedir".

Fix:

U must turn off "directory listing" in properties:

change 12(LR) to 4(read).

2. WinApache for Explorer

Don't confuse with Apache(win32) web server.

This is update for Explorer, that allows it to be web server

(!!). I don't no where you can download it, because i founded this update on disk.

Exploit:

<http://www.anyhost.com/dll/main.dll://test.exe?test=anylocation>

This url will freeze the web server and all files & folders become read-accessable for nobody.

Fix:

Don't use this sh**... and download Apache Web Server.

3. mIRC32 v6.* K.Mardam-Bey

Bug founded in function `$exists()`.

How does it function work?

From mIRC help:

`$exists(file/dir)`

Returns `$true` if a file or dir exists and `$false` if it doesn't.

`$exists(c:\mirc\mirc.exe)` – returns `$true` or `$false`.

How does it bug work?

VulnWatch: [VulnWatch] 5 bugs

If the name of checked file\dir will be "aux", function will return \$true.

Example:

\$exists(c:\mirc\aux.blablabla) – returns \$true (but really it must be \$false, because file doesn't exist)

4. XiRCON v.1.0B4.

Dot bug in sound-requests.

If you want to use this function (play sound-requests), you must turn it ON in properties and set the "play dir" (directory with ur music-files). XiRCON's authors thought, that remote user can't play files from another directories. It's fault.

By using this command:

```
/ctcp <nick> sound ..\..\..\any.wav
```

we can play any sound files on remote host.

Example (for XP):

```
/ctcp <nick> sound ..\..\..\..\windows\media\town.mid
```

Remote user will listen funny song => (1 min 19 sec).

5. KDE v.3.*

Buffer overflow in file kdeCMD.

Exploits:

```
./kdeCMD -f [129b] – system crash
```

```
./kdeCMD -f [128b] + [shellcode] – local root
```

Bug exists in all versions, that have file