

[NT] Multiple Heap Overflows in FTP Desktop

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0030.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/03

To: list@securiteam.com

Date: 14 Sep 2003 15:55:42 +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>

Multiple Heap Overflows in FTP Desktop

SUMMARY

" <<http://www.ftpdesktop.com>> FTP Desktop lets you access FTP sites as if they were folders on your computer. Now you can move your files between your hard disk and remote FTP sites with greater ease".

It is possible to cause multiple heap overflows in FTP Desktop, allowing modification of the EIP pointer – this allows a remote attacker to cause the program to execute arbitrary code.

DETAILS

Vulnerable systems:

* FTP Desktop version 3.5 and prior

Examples:

FTP Banner:

(FTP Desktop connected...)

```
PADDING EBP EIP
220 [229xA][4xB][4xX]
```

(Access violation when executing 0x58585858) // 4xX

Securiteam: [NT] Multiple Heap Overflows in FTP Desktop

Username:
(FTP Desktop Sends 'USER username')

PADDING EBP EIP
331 [229xA][4xB][4xX]

(Access violation when executing 0x58585858) // 4xX

Password:
(FTP Desktop Sends 'PASS password')

PADDING EBP EIP
331 [229xA][4xB][4xX]

(Access violation when executing 0x58585858) // 4xX

Vendor status:
The vendor has been informed, and they are fixing this bug. The updated version, when released, can be downloaded from:
<<http://www.ftpdesktop.net/download.html>>
<http://www.ftpdesktop.net/download.html> (
<<http://www.ftpdesktop.net/download/ftpsetup.exe>>
<http://www.ftpdesktop.net/download/ftpsetup.exe>).

ADDITIONAL INFORMATION

The information has been provided by <mailto:b_naamneh@hotmail.com> Bahaa Naamneh.

=====

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.