

# [REVS] Manipulating FTP Clients Using the PASV Command

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00017.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 5 Mar 2007 19:56:32 +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>

-----

Manipulating FTP Clients Using the PASV Command

---

## SUMMARY

This paper discusses a common implementation flaw in the File Transfer Protocol (FTP). Several popular FTP clients are affected including web browsers. Some proof of concept code is presented to demonstrate how the vulnerability can be used to extend existing JavaScript-based port scans. Finally, some consideration is given to other ways in which this flaw could present a security risk to other FTP clients.

## DETAILS

Vulnerable FTP Clients:

The following web browsers have been found to respond to malformed PASV responses in the way described above:

- \* Firefox 1.5.0.9
- \* Firefox 2.0.0.2
- \* Opera 9.10
- \* Konqueror 3.5.5

Several command line FTP clients have also been found to be vulnerable. However as the vendors have not been notified (and the author cannot think

## [REVS] Manipulating FTP Clients Using the PASV Command

of an interesting way of exploiting command line clients), they have been omitted from this paper.

### Immune FTP Clients

The following web browsers seem to ignore the IP address returned in PASV responses. They simply connect to the IP address to which the original control connection (21/TCP) was made:

- \* Microsoft Internet Explorer 7.0.5730.11
- \* Microsoft Internet Explorer 6.0.3790.0

### FTP Client Implementation Flaw

It is possible for malicious FTP servers to cause some popular FTP clients to connect to TCP ports on other hosts. This allows us to extend existing JavaScript-based port scan techniques [spi] in the follow ways:

- \* Scan ports which modern browsers would not normally connect to [portban]
- \* Fingerprint services which do not send a banner by timing how long the server takes to terminate the connection
- \* Perform simple banner grabbing to identify services running on other hosts

### Vendor Responses:

No response was provided by either Mozilla or Opera.

KDE responded and discussed both issues. However, they have yet to be convinced of the severity of the FTP PASV Vulnerability. Unfortunately, providing POC to demonstrate banner grabbing was made harder (impossible?) by the crash during the reading of child FTP iframes. KDE have reproduced the crash and produced a patch [konqcrash].

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:mark@xxxxxxxxxxxxxx>> mark.

The original article can be found at:

<<http://bindshell.net/papers/ftppasv/ftp-client-pasv-manipulation.pdf>>

<http://bindshell.net/papers/ftppasv/ftp-client-pasv-manipulation.pdf>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

## [REVS] Manipulating FTP Clients Using the PASV Command

### 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.