

# [NEWS] Raptor Firewall FTP Bounce Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0070.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 04/17/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Wed, 17 Apr 2002 20:38:11 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Raptor Firewall FTP Bounce Vulnerability

---

## SUMMARY

The Raptor Firewall can make an FTP server behind it vulnerable to the well-known FTP bounce vulnerability even if the FTP server used is not susceptible to this issue.

## DETAILS

Environment:

Firewall: Raptor 6.5.3i on Sun Solaris 7

FTP Server: wu-ftp on internal network with anonymous access

Configuration: Using built-in Raptor FTP proxy for inbound FTP access from Internet

Details:

While performing a penetration test for a customer, we discovered that their FTP server was vulnerable to the well-known FTP Bounce attack from the Internet. However, subsequent conversation with the customer showed that the FTP server itself (a recent version of wu-ftp) was not vulnerable to the FTP bounce attack.

It appears that the Raptor Firewall's FTP proxy was somehow making the FTP server vulnerable to the FTP bounce vulnerability even though the FTP server itself was immune to this problem.

## Securiteam: [NEWS] Raptor Firewall FTP Bounce Vulnerability

The Firewall vendor (Symantec) has been informed of this issue.

Analysis:

We verified and analyzed the vulnerability using the following setup:

1. "attacker" – A Linux system on the Internet that connects to the FTP server and exploits the vulnerability.
2. "victim" – A second Linux system on the Internet that is the target of the bounce attack.
3. "server" – The FTP server. External address 194.217.26.147, internal 10.1.13.5.
4. "Firewall" – The Raptor Firewall.

We verified the FTP bounce vulnerability from the Internet and used the "tcpdump" packet sniffer on the Internet "attacker", the Internet "victim" (target of the ftp bounce test), and the FTP server to determine what was going on.

It turns out that the Raptor Firewall re-writes the inbound FTP "PORT" command and changes the IP address to be the Hacker's IP rather than the Victim's, and the port number to be another ephemeral port. This means that the FTP server cannot detect the FTP bounce attack because it sees the correct IP address (the one of the hacker rather than the victim) and an ephemeral port. However, when the FTP Server makes the outbound connection to this IP address and port, the Firewall re-writes the IP address and port in the packet to be the IP address and port of the victim that was originally specified by the Hacker.

Thus, the Raptor Firewall prevents the FTP Server from detecting the FTP bounce attack, and permits the attack to take place. Because the FTP Server will always see the "correct" IP address and port in the PORT command, it cannot determine that an FTP bounce attack is being carried out and will accept the command.

Further information:

Further information, including annotated "tcpdump" packet traces are available at:

<<http://www.nta-monitor.com/news/raptor-set.htm>>

<http://www.nta-monitor.com/news/raptor-set.htm>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[Roy.Hills@nta-monitor.com](mailto:Roy.Hills@nta-monitor.com)>  
Roy Hills.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

Securiteam: [NEWS] Raptor Firewall FTP Bounce Vulnerability

=====  
=====

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.

- 
- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[\[NT\] Microsoft IIS Vulnerabilities in Cisco Products](#)"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)