

# [UNIX] SafeTP Reveals Internal Server IP Addresses

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0102.html>

---

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

*Date:* 09/30/02

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

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

Date: Mon, 30 Sep 2002 09:42:04 +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.

-----

SafeTP Reveals Internal Server IP Addresses

---

## SUMMARY

<<http://safetp.cs.berkeley.edu>> SafeTP is a revolutionary new security application for Windows and UNIX users who use FTP (File Transfer Protocol) to connect to their accounts on UNIX or NT/2000 FTP servers. A security vulnerability in the product allows remote attackers to cause the product to reveal sensitive IP information about the internal network/hosts.

## DETAILS

The basic problem is that any SafeTP client can get the SafeTP server to cough up an internal IP address if passive mode transfers are required in a NAT environment. For example, check out the "227 Entering Passive Mode (10,7,34,85,5,133)" entry in the log below. (169.229.60.94 is the public/external IP address -- 10.7.34.85 is the internal IP address.)

```
D:\OSOmissions\snort\rules>ftps safetp.nowhere.com
220-SafeTP: Negotiating FTP connection...
220-safetp.nowhere.com X2 WS_FTP Server 3.1.0 (1506847632)
220-Changed to Protect the Innocent
220-safetp.nowhere.com X2 WS_FTP Server 3.1.0 (1506847632)
```

## Securiteam: [UNIX] SafeTP Reveals Internal Server IP Addresses

```
220-*** This server can accept secure (encrypted) connections. ***
220-*** See http://safetp.cs.berkeley.edu for info. ***
220 SafeTP: Control channel secure: X-SafeTP1. Data channel secure.
PBSZ=32801b
Connected to safetp.nowhere.com.
User: SomeUser
331 Password required
Password: *****
230-user logged in
230-Hello Some User. Welcome to the SafeTP File Transfer System!
230 user logged in
ftp> ls
200 PORT command ok.
Timed out waiting for connection from server.
ftp> passive
Passive mode On .
ftp> ls
425 Failed to connect to 192.168.3.162, port 3303: connect: Connection
timed out
(code 10060)
ftp> passive
Draining: 510 Assertion failed: ftpd reply: 150 Opening ASCII data
connection for directory listing
Draining: 227 Entering Passive Mode (10,7,34,85,5,133).
Passive mode Off .
ftp> put tendot.txt
227 Entering passive mode (169,229,60,94,156,186).
150 Opening ASCII data connection for tendot.txt
226 transfer complete
ftp: 1094 bytes sent in 0.98Seconds 1.09Kbytes/sec.
ftp> quit
221-Good-Bye
221-Goodbye Some User. Thank you for visiting the SafeTP File Transfer
System!
221 Good-Bye
```

### Vendor status:

Jonathan sent email messages to all the listed support contacts (Dan Bonachea – Windows software – [bonachea@cs.berkeley.edu](mailto:bonachea@cs.berkeley.edu) and Scott McPeak – UNIX software – [smcpeak@cs.berkeley.edu](mailto:smcpeak@cs.berkeley.edu)), and asked another long-time user to do the same. Neither of us got any response after a few weeks.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:jonathan@stdnet.com>>  
Jonathan G. Lampe.

=====

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:

Securiteam: [UNIX] SafeTP Reveals Internal Server IP Addresses

[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)

=====  
=====

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): "[EXPL] Local Root Exploit Found in gds\_lock\_mgr"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)