

# [NT] TwinFTP Server Directory Traversal Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0026.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/14/04

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

Date: 14 Sep 2004 13:45:14 +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>

-----

TwinFTP Server Directory Traversal Vulnerability

---

## SUMMARY

<<http://www.twinfo.com/>> TwinFTP Server is an FTP server released by Jigunet Corporation for the Windows platform.

A vulnerability exists in TwinFTP server that allows a malicious user access files outside the FTP directory. This vulnerability may also be exploited to bypass directory restrictions enforced by the FTP server to write arbitrary files into directories that the server process has access to.

## DETAILS

### Vulnerable Systems:

- \* TwinFTP Server Standard Version 1.0.3 R2 (Win32)
- \* TwinFTP Server Enterprise Version 1.0.3 R2 (Win32)
- \* TwinFTP Server Standard/Enterprise Version 1.0.3 R3 released before 10 Sep 2004

### Immune Systems:

- \* TwinFTP Server Standard Version 1.0.3 R3 (Win32), released on 10 Sep

## Securiteam: [NT] TwinFTP Server Directory Traversal Vulnerability

2004. is vulnerable.

A directory traversal vulnerability exists in several FTP commands of TwinFTP that may be exploited by a malicious user to access files outside the FTP directory. The problem lies with the incorrect filtering of directory name supplied to CWD, STOR and RETR commands. Directory traversal is possible when the directory name contains three dots and a forward slash, e.g. ".../winnt".

This vulnerability may be exploited to bypass directory restrictions enforced by the FTP server to write arbitrary files into directories that the server process has access to. This is critical since it may be abused by malicious users to overwrite system files within the Windows directory if the TwinFTP server runs with Administrator privilege.

### Solution:

Upgrade to Version 1.0.3 R3 that is released on 10 September 2004. Version 1.0.3 R3 which was released before 10 September 2004 is partially vulnerable in RETR and STOR commands.

### Disclosure Timeline:

02 Aug 04 – Vulnerability Discovered

04 Aug 04 – Initial Vendor Notification (no reply)

09 Aug 04 – Second Vendor Notification

13 Aug 04 – Vendor released Version 1.0.3 R3 which fixes directory traversal problem, but RETR and STOR commands are still vulnerable.

13 Aug 04 – Notified vendor about RETR and STOR vulnerability (no reply)

30 Aug 04 – Second vendor notification about RETR and STOR vulnerability

10 Sep 04 – Vendor re-released Version 1.0.3 R3 which fixes RETR and STOR commands.

12 Sep 04 – Public Release

### ADDITIONAL INFORMATION

The information has been provided by <mailto:chewkeong@security.org.sg>  
Chew Keong TAN.

The original article can be found at:

<<http://www.security.org.sg/vuln/twinftp103r2.html>>

<http://www.security.org.sg/vuln/twinftp103r2.html>

=====

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.

## Securiteam: [NT] TwinFTP Server Directory Traversal Vulnerability

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.