

[NT] Total Commander WCX_FTP.INI FTP Account Information Weak Encryption

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00016.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Dec 2005 16:05:12 +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>

Total Commander WCX_FTP.INI FTP Account Information Weak Encryption

SUMMARY

" <<http://www.ghisler.com/>> Total Commander is a file manager for Windows, a program like Windows Explorer to copy, move or delete files. However, Total Commander can do much more than Explorer, e.g. pack and unpack files, access ftp servers, compare files by content, etc"

" <<http://securityresponse.symantec.com/avcenter/venc/data/w32.gudeb.html>> W32.Gudeb is a worm that lowers security settings and hides folders on the compromised computer. It spreads via FTP and gathers valid accounts from Total Commander configuration file."

Weak password storage by Total Commander's settings file, allows local attackers and Worms to gain FTP login information and compromise other systems.

DETAILS

Vulnerable Systems:

- * Total Commander version 6.53

[NT] Total Commander WCX_FTP.INI FTP Account Information Weak Encryption

Total Commander file manager/FTP client utility is confirmed as affected to weak account information encryption vulnerability. The vulnerability is caused due to weak encryption algorithm used when internal FTP account information is saved to the configuration file WCX_FTP.INI. Both username and password are saved to the file located at directory from %System% variable.

This is reportedly being exploited by a new W32.Gudeb worm. W32.Gudeb spreads via FTP and gathers valid accounts from Total Commander configuration file. This malware searches for the file %System%\WCX_FTP.INI and gathers valid username and password details. If this operation is successful, it will reportedly upload a copy of itself to the newly compromised computers.

Example:

```
C:\WINNT\wcx_ftp.ini:
---clip---
[OldConnections]
0=ftp.removed.com
[connections]
1=Homepage
[Homepage]
host=ftp.removed.com
username=www.removed.fi
password=CF6ECD90B708F354B2CF41AAA833 (*)
directory=/pictures
---clip---
```

*) the content of the password field changed due to security/privacy reasons

Workaround:

Do not save FTP connections.

Disclosure Timeline:

- 02-Dec-2005 – Vulnerability researched and confirmed
- 03-Dec-2005 – Detailed research, new FTP hosts tested
- 03-Dec-2005 – Vendor contacted, workaround delivered to the vendor
- 03-Dec-2005 – Security companies and several CERT units contacted

ADDITIONAL INFORMATION

The information has been provided by <<mailto:juha-matti.laurio@xxxxxxxxx>>
Juha-Matti Laurio.

=====

[NT] Total Commander WCX_FTP.INI FTP Account Information Weak Encryption

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.

-
- Prev by Date: [*\[NT\] Schneier's PasswordSafe Password Validation Flaw*](#)
 - Next by Date: [*\[NEWS\] Dell TrueMobile 2300 Wireless Broadband Router Authentication Bypass*](#)
 - Previous by thread: [*\[NT\] Schneier's PasswordSafe Password Validation Flaw*](#)
 - Next by thread: [*\[NEWS\] Dell TrueMobile 2300 Wireless Broadband Router Authentication Bypass*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)