

# [NT] Crystal FTP Pro Client LIST Buffer Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0053.html>

---

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

**Date:** 12/19/04

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

Date: 19 Dec 2004 19:49:54 +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>

-----

Crystal FTP Pro Client LIST Buffer Overflow

---

## SUMMARY

<<http://www.casdk.com/>> Crystal FTP Pro is "a Top awarded FTP client for dummies and experts". A vulnerability in the way Crystal FTP Pro parses incoming LIST responses allows a remote attacker to cause the program to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* Crystal FTP Pro version 2.8

Crystal FTP Pro client, does not perform bound checking on the results returned by 'LIST' command. A malicious ftp server, could execute arbitrary code on the target user's client, replies to a 'LIST' command request with a file list that contain a long file extension.

Example:

le.AAAAAAAAAAAAAA...(over 250 characters)

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:luca.ercoli@inwind.it>> Luca

Securiteam: [NT] Crystal FTP Pro Client LIST Buffer Overflow

Ercoli.

=====

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)

=====  
=====

**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.