

[NT] Buffer Overflow in Whisper FTP Surfer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/20/04

To: list@securiteam.com

Date: 20 Jul 2004 10:01:01 +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>

Buffer Overflow in Whisper FTP Surfer

SUMMARY

<<http://www.whispertech.com/>> Whisper FTP Surfer is "a freeware FTP client for Windows". A buffer overflow occurs when trying to open a file with a long name from an FTP Server.

DETAILS

Vulnerable Systems:

- * Whisper FTP Surfer version 1.0.7

For common extension (as .txt) FTP Surfer create a temporary file and tries to open it. When closing the FTP Surfer, it tries to delete the temporary file. The long name of the file added to the name of the temporary folder overflows the buffer.

Proof of concept:

Create a file with a very long name with the ".txt" extension, put it on an FTP Server and try to open it from FTP Surfer, you'll get an error message: "Unable to execute program". Then when you close the FTP Surfer the EIP will be invalid.

ADDITIONAL INFORMATION

Securiteam: [NT] Buffer Overflow in Whisper FTP Surfer

The information has been provided by <mailto:giocasati@interfree.it>
Komrade.

=====

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.