

[NT] WS_FTP SITE CPWD Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0033.html>

From: support@securiteam.com

Date: 08/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 10 Aug 2002 22:41:17 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

WS_FTP SITE CPWD Buffer Overflow Vulnerability

SUMMARY

WS_FTP Server is a widely used FTP Server for the Microsoft NT/2000/XP platform. There exists a vulnerability within the software, which allows an attacker to overwrite the return address on the stack, thus taking control of the execution flow. This allows the attacker to run arbitrary code on the system remotely.

DETAILS

Vulnerable systems:

- * WS_FTP Server version 3.1.1

The WS_FTP Server allows users to change their password through a site command, "site cpwd". The code handling the argument supplied with this site command contains an unchecked string copy, allowing an attacker to overwrite the return address stored on the stack. Since the WS_FTP Server is running as a service, in most cases it will be executing as SYSTEM.

The feature to allow user to change their passwords is enabled by default, but it is possible for a WS_FTP Server administrator to turn this functionality off.

Securiteam: [NT] WS_FTP SITE CPWD Buffer Overflow Vulnerability

Vendor response:

This issue was reported to Ipswitch on July 25, 2002 and a patch was produced short thereafter.

Recommendation:

Install the patch provided by Ipswitch:

ftp://ftp.ipswitch.com/ipswitch/product_support/WS_FTP_Server/ifs312.exe
ftp://ftp.ipswitch.com/ipswitch/product_support/WS_FTP_Server/ifs312.exe

For more info, see:

http://www.ipswitch.com/Support/WS_FTP-Server/patch-upgrades.html
http://www.ipswitch.com/Support/WS_FTP-Server/patch-upgrades.html

Also, consider turning off all unused features and run the software under a less privileged account.

ADDITIONAL INFORMATION

The information has been provided by <mailto:andreas@atstake.com> Andreas Junestam.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Opera FTP View Cross-Site Scripting Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)