

[EXPL] ArGoSoft FTP Server Buffer Overflow Exploit (DELE)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0030.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/05/05

To: list@securiteam.com

Date: 5 Apr 2005 16:44:18 +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>

ArGoSoft FTP Server Buffer Overflow Exploit (DELE)

SUMMARY

<<http://www.argosoft.com/>> ArGoSoft FTP Server is "a lightweight FTP Server for Microsoft Windows platforms"

ArGoSoft FTP server contains a remote buffer overflow in the DELE (delete) command, that may cause execution of arbitrary machine code. The following exploit is a proof of concept to the previously mentioned buffer overflow vulnerability in ArGoSoft FTP Server.

DETAILS

Vulnerable Systems:

* ArGoSoft versions 1.4.2.29 and prior

Exploit:

/*

ArGoSoft Ftp Server remote overflow exploit

author : c0d3r "kaveh razavi" c0d3rz_team@yahoo.com c0d3r@ihsteam.com

package : ArGoSoft 1.4.2.29 and prior

advisory : packetstormsecurity.nl/0503-advisories/argosoftFTP1428.txt

Securiteam: [EXPL] ArGoSoft FTP Server Buffer Overflow Exploit (DELE)

company address : argosoft.com

the bug was found by a mate and reported to argosoft and they released another version . I downloaded the patched ver at www.argosoft.com and started to test the server . I saw that they worked with the vul but they didnt solve the mentioned DELE overflow . he did a wise job every long char which would be send to server it will write a nullbyte in the middle so we cant overwrite eip or other registers normally .

The eip would be overwrite like 00410041 which seems useless . the server

wont crash but it shows that it has beed overflowed . but the program maker

doesnt think there are people who can do wiser job ! well there is a way to

get shell.I just mention it.the code below is just show that the server is vuln.

we can overwrite eip with a nullbyte without sending a null !!!

so think there is a jmp call pop push register is around 004400E1 (for example)

so we can directly jmp to anywhere we want . anyway if u want u can try

=====

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.