

# [NT] Multiple Vulnerabilities in 602Pro LAN SUITE 2003 (Incorrect File Permissions, File Reading)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0087.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 09/29/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 29 Sep 2003 11:04:37 +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>

-----

Multiple Vulnerabilities in 602Pro LAN SUITE 2003 (Incorrect File Permissions, File Reading)

---

## SUMMARY

<<http://www.software602.com/products/ls/>> 602Pro LAN SUITE is "an easy-to-install and manage all-in-one server application. Its standards-based SMTP/POP3 e-mail server provides effective e-mail communication without the risk of destructive virus infiltration and productivity robbing unsolicited e-mail. Fax services seamlessly integrate into user mailboxes to unify e-mail and fax message access".

Multiple vulnerabilities have been discovered in the product allowing remote attackers to view sensitive log files, and read any arbitrary files.

## DETAILS

Vulnerable systems:

\* 602PRO LAN SUITE 2003, build 2003.0.3.0828

Multiple vulnerabilities in the LAN SUITE 2003 software (WebMail interface) which allow attackers to view sensitive information about users

## Securiteam: [NT] Multiple Vulnerabilities in 602Pro LAN SUITE 2003 (Incorrect File Permissions, File Reading)

(Mailbox number, Message ID, Login Time etc...) and read any file on the server.

### Sensitive Files Exposure

When a user logs in to LAN SUITE 2003 WebMail server, m602cl3w.exe will create a temporary file and folder holding sensitive information about the current user and they are accessible through the LAN SUITE WebMail interface <http://www.victim.com/mail/>. Tempdirs.lst file holds the temporary folder name of current users. The temporary folder contains two files named MSGlist.mid and MSGlist.mil. Messages ID are written to MSGlist.mid file. The username and mailbox number are written to MSGlist.mil.

Log files are also accessible by anyone at:

<http://www.victim.com/mail/S030904L.LOG> (YY/MM/DD). Attacker might gain sensitive information of username, user's IPs, login time etc... This information could be useful to assist in further exploit once they obtained the file.

### Arbitrary File Reading

Malicious user can read any file on the server if they have a valid LAN SUITE WebMail username and password. M602cl3w.exe does check for dot-dot-slash most of the time but not when the action "GetFile" is used. For example, a malicious user can read the boot.ini file by sending a request like this:

<http://www.victim.com/mail/m602cl3w.exe?A=GetFile&U=7921604D7A587937986E24242C0588&DL=0&FN=../../../../>

Where "U" is the current user handle's string. Malicious users can also read other user's mails by using the information they got from exploiting the first vulnerability.

For example:

<http://www.victim.com/mail/m602cl3w.exe?A=GetFile&U=7921604D7A587937986E24242C0588&DL=0&FN=../../../../>

Vendor status:

You can obtain a patch for the above vulnerabilities at

<<http://download3.software602.com/ls2003.exe>>

<http://download3.software602.com/ls2003.exe>.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:dphuong@yahoo.com> Phuong Nguyen.

=====

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.