

# [NT] WinWrapper Professional Remote File Disclosure Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0097.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/26/01

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Subject: [NT] WinWrapper Professional Remote File Disclosure Vulnerability

Message-Id: <20010826062503.E270A138BF@mail.der-keiler.de>

Date: Sun, 26 Aug 2001 08:25:03 +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.

-----

## WinWrapper Professional Remote File Disclosure Vulnerability

---

### SUMMARY

<<http://www.ant.co.jp/Products/Wrapperpro2.htm>> WinWrapper Professional is a firewall software. It provides Web-based remote console, which suffers from a vulnerability allowing remote attackers to read arbitrary files on the system.

### DETAILS

Vulnerable systems:

WinWrapper Professional version 2.0

Immune systems:

WinWrapper Professional version 2.0.1

WinWrapper Professional is a firewall software that is developed by ASCII NT, INC. It is designed to protect WindowsNT/2000 systems, and provides additional Web-based capability of remote administration. Nevertheless, the program that is used as remote administration server contains a vulnerability that makes it possible to read arbitrary files on the target

## Securiteam: [NT] WinWrapper Professional Remote File Disclosure

system with Local System context.

Example:

<http://>:4096/../../../../winnt/repair/sam>

Note:

The port number 4096 (TCP) is the default port number used by the product.

Patch information:

A fixed module (Ver.2.0.1) is available from the following URL:

<<http://www.tsc.ant.co.jp/products/download.htm>>

<http://www.tsc.ant.co.jp/products/download.htm>

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:y.arai@lac.co.jp>> ARAI Yuu (LAC).

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Hotmail LINK CSS Vulnerability (New Strain)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)