

[NT] Web Traversal Vulnerability in PCI NetSupport Manager

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0095.html>

From: support@securiteam.com

Date: 03/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 23 Mar 2002 16:59:24 +0100 (CET)

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.

Web Traversal Vulnerability in PCI NetSupport Manager

SUMMARY

PCI are the developers of the NetSupport range of award winning solutions; comprising of powerful Remote Control, Enterprise Management and IT Training products. One of its products [<http://www.pci.co.uk/nsm/remote_control.htm>](http://www.pci.co.uk/nsm/remote_control.htm) NetSupport Manager allows remote attackers to access files that reside outside the normally bounding HTML root directory.

DETAILS

Vulnerable systems:

PCI NetSupport Manager versions up to 7.0

Immune systems:

PCI NetSupport Manager version above 7.0

It is possible to view and download files on machines running PCI NetSupport Manager that have the web extensions switched on (default port 80).

Securiteam: [NT] Web Traversal Vulnerability in PCI NetSupport Manager

Example on a standard version 5.5 install (location c:\nsm) the URL to view the boot.ini file in the root would be:

http://machinename:relevant_port/././boot.ini

Version 6 and above:

http://machinename:relevant_port/././boot.ini

ADDITIONAL INFORMATION

The information has been provided by <mailto:watcher60@hotmail.com>
watcher60.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] www.myownemail.com Vulnerable to Cross Site Scripting"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)