

[NEWS] Sybex E-Trainer Directory Traversal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0086.html>

From: support@securiteam.com

Date: 02/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 15 Feb 2002 03:55:22 +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.

Sybex E-Trainer Directory Traversal Vulnerability

SUMMARY

<<http://www.sybextrainer.com/FrontDoor/0.1076.3-23.00.html>> Sybex E-Trainer's are computer based training courses. They run through a web interface using your web browser. When you launch the course, it loads its own web server and launches your default web browser that connects to you locally on the default HTTP server port, 80. When you close your browser, the web server also shuts down. A security vulnerability in the product allows remote attackers to traverse and access files that reside outside the normal bound HTML root directory.

DETAILS

The vulnerability that takes place is the infamous ".." directory traversal. With a specially crafted request to the web server you can view any file on the target's computer under the logged in users permissions. The request is in the format of:

<http://target/netget?sid=user/../../filename.ext>

The web server only runs when a user runs the e-trainer course. When the user closes the browser, the web server also shuts down. However if the

Securiteam: [NEWS] Sybex E-Trainer Directory Traversal Vulnerability

user opens the e-trainer and uses the same browser window to start browsing other websites, the web server will stay open. This could cause the vulnerable server to continue on running for an even a longer time. It should also be noted that this web server has not logging features and it is open to any connection requests. Not just from the local host.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ZeroBreak@softhome.net>
ZeroBreak.

=====

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: "[UNIX] Bad Temporary File Handling in GNAT"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)