

[UNIX] Arbitrary File Disclosure Vulnerability in Sympoll

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0138.html>

From: support@securiteam.com

Date: 07/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 31 Jul 2002 13:29:04 +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.

Arbitrary File Disclosure Vulnerability in Sympoll

SUMMARY

<<http://www.ralusp.net/heterodox/sympoll.php>> Sympoll is a customizable voting booth system. It is written using PHP and requires access to a MySQL database. A security vulnerability in the product allows remote attackers to read the content of arbitrary files.

DETAILS

Vulnerable systems:

- * Sympoll version 1.2

Immune systems:

- * Sympoll version 1.3

A missing variable integrity check allows arbitrary files to be viewed on a web server that hosts Sympoll. Hosts that have disabled the `register_globals` directive in their `php.ini` file are not at risk.

Vendor status:

This vulnerability was reported to the Sympoll author on Tuesday, July 30 2002 at approximately 13:45 EST. A new version with a verified fix was

Securiteam: [UNIX] Arbitrary File Disclosure Vulnerability in Sympoll

released by 16:15 EST the same day. It can be downloaded from
<<http://www.ralusp.net/sympoll/>> <http://www.ralusp.net/sympoll/>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ralusp@mail.com>> David Raeman.

=====

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] Directory Traversal vulnerability in [sendform.cgi](#)"
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)