

[UNIX] PHP fopen() Warning Cross-Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0077.html>

From: support@securiteam.com

Date: 07/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 18 Jul 2002 07:31:53 +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.

PHP fopen() Warning Cross-Site Scripting Vulnerability

SUMMARY

PHP's fopen() function warning output has been found to inadequately filter out malicious content, this makes it prone to an XSS security vulnerability.

DETAILS

Systems Affected:

Any PHP interpreter configured to use error output, and to recognize warnings as errors; system must host a script-allowing user to open arbitrary file.

Technical Description:

PHP's default configuration is to display error output in the browser. It is also configured by default to print out warning messages.

A vulnerability in the way fopen()'s warnings are handled may cause a cross-site scripting vulnerability.

Demo script:

fo-xss.php:

Securiteam: [UNIX] PHP fopen() Warning Cross-Site Scripting Vulnerability

```
<?php $handle = fopen($xssvar); ?>
```

If your system is running a default PHP configuration, this script will return \$xssvar unchanged to the user.

NOTE: This sample requires register_globals to be on.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mattmurphy@kc.rr.com>
Matthew Murphy.

=====

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] Wiki Module PostNuke Cross-Site Scripting Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)