

[UNIX] PHPProxy Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0093.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 11:37:55 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

PHPProxy Cross Site Scripting

SUMMARY

<<http://www.whitefyre.com/poxy/>> PHPProxy is "a web HTTP (for now; FTP is not supported yet) proxy programmed in PHP designed to bypass firewalls and other proxy restrictions through a web interface very similar to the popular CGIProxy".

A vulnerability in the PHPProxy's handling of incoming user provided data allows an attacker to use the PHP script for a cross site scripting vulnerability.

DETAILS

Vulnerable Systems:

* PHPProxy version 0.3 and prior

There is exists an XSS vulnerability where a malicious user could inject any evil HTML tags or JavaScript into PHPProxy's web page. The vulnerability can be exploited by putting arbitrary code in 'error' parameter of the PHPProxy program.

Example:

<http://vulnerable/poxy/index.php?error=html%20code%20could%20be%20easily%20injected%20here>

Securiteam: [UNIX] PHPProxy Cross Site Scripting

ADDITIONAL INFORMATION

The information has been provided by <mailto:boshcash@msn.com> Boshcash.

=====

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.