

[UNIX] PHP-Ping Arbitrary Command Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0092.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/29/03

To: list@securiteam.com

Date: 29 Dec 2003 18:24:03 +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>

PHP-Ping Arbitrary Command Execution

SUMMARY

<<http://www.theworldsend.net/>> PHP-Ping is "a simple ping utility written in PHP". A vulnerability in the script allows remote attackers to cause the script to execute arbitrary code.

DETAILS

Due to improper filtering of the count variable, a remote attacker can insert arbitrary commands into the command executed by the PHP script (the ping command).

Example:

You can use one of the following to verify whether your system is vulnerable or not:

<http://www.example.com/php-ping.php?count=1+%26+ls%20-1+%26&submit=Ping%21>

<http://www.example.com/php-ping.php?count=1+%26+cat%20/etc/passwd+%26&submit=Ping%21>

Solution:

Add the following (proper) filtering lines:

```
// replace bad chars
$host= preg_replace ("[/^A-Za-z0-9.]"/,"",$host);
$count= preg_replace ("[/^0-9.]"/,"",$count);
```

Securiteam: [UNIX] PHP-Ping Arbitrary Command Execution

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@ppp-design.de>
ppp-design.

=====

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.