

[UNIX] SCO OpenServer Xsco Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0043.html>

From: support@securiteam.com

Date: 06/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 11 Jun 2002 22:25:33 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

SCO OpenServer Xsco Heap Overflow

SUMMARY

The SCO OpenServer Xsco application is installed setuid root by default.

The application has been found to contain the same heap overflow that

<<http://www.securiteam.com/unixfocus/5FP0E0K40W.html>> Xsun has.

DETAILS

Vulnerable systems:

- * SCO/Caldera OpenServer 5.x

Impact:

If properly exploited the following could be used to take root on the server with the Xsco binary.

Example:

```
bash-2.03$ ./Xsco :1 -co <b0f here> -crt /dev/console
```

```
Tue Jun 11 10:32:59 2002
```

```
Couldn't open RGB_DB 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
...
```

```
Segmentation Fault
```

Securiteam: [UNIX] SCO OpenServer Xsco Heap Overflow

```
0x8164073 in _grantpt ()  
(gdb) bt  
#0 0x8164073 in _grantpt ()  
#1 0x8164532 in malloc ()  
#2 0x80027103 in _s_a_get ()  
#3 0x81594bc in _ptsname ()  
#4 0x8087526 in wctype ()  
#5 0x8085e95 in wctype ()  
#6 0x80745f4 in wctype ()  
#7 0x804d69b in wctype ()
```

```
(gdb) i r  
eax 0x41414141 1094795585  
ecx 0x495b38d4 1230715092  
edx 0x0 0  
ebx 0x18 24  
esp 0x8045814 0x8045814  
ebp 0x8045834 0x8045834  
esi 0x41414140 1094795584  
edi 0x819f794 135919508  
eip 0x8164073 0x8164073
```

Solution:

The vendor was notified and is working on a fix. A working workaround is at the moment unavailable.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dotslash@snoosoft.com>> KF.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Multiple Security Issues in Geeklog (XSS, SQL Inject)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)