Full Disclosure works, here's proof:

From: cklaus () shadow net (Christopher Klaus)
Date: Thu, 1 Dec 94 1:07:42 EST

```
Besides Spaf's argument that full disclosure has no proof of being
productive, I think almost everyone I talked with who works in security
for their vendor agreed that they try to fix security holes as soon as
possible, and ones that have been publicly disclosed, would take higher
priority in the list of patches to create.  Only a real bloated and
beaucratic organization wouldn't make patches ASAP when customers are
screaming for them.

Anyways, it has been less than a week and here's SCO patches.  If 8LGM
had only reported the bugs to CERT and SCO, who knows how long would we
have seen the patches?

============================================================================
                            SCO Advisory 94:001
                            November 30th, 1994
        Patches for at(C), login(M), prwarn(C), sadc(ADM), pt_chmod
----------------------------------------------------------------------------

The Santa Cruz Operation has been informed of the following problems present
in our software.

I.   Description

     The programs at(C), login(M), prwarn(C) sadc(ADM), and pt_chmod
     may each allow unauthorized root access to the system.

     There are four unrelated issues present, one for each program listed
     above.


II.  Impact

     Any user with an account on the system may obtain root access using
     any one of the programs listed.


III. Releases

     These problems exist on the following releases of SCO Products:

        SCO Unix System V/386 Release 3.2 Versions 4.2, 4.1, and 4.0
        SCO Open Desktop Lite Release 3.0
        SCO Open Desktop Release 3.0 and 2.0
        SCO Open Server Network System Release 3.0
```

SCO Open Server Enterprise System Release 3.0

IV. Solution

SCO is providing the following (S)ystem (S)ecurity (E)nhancements, SSEs, to address these problems. These are preliminary patches which SCO feels addresses the issues at hand, but these patches have not been fully tested and integrated and hence cannot officially be supported. Official patches should be available in the near future via a (S)upport (L)evel (S)upplement. (SLS). The README file mentioned below will be updated when an official Supplement is available.

Binary	Patch
at(C)	sse001
login(M)	sse002
prwarn(C)	sse003
sadc(ADM)	sse004
pt_chmod	sse005

These are available at the following sites:

Anonymous ftp: ftp.sco.COM:/SSE

UUCP downloading, and SOS access: sosco (USA), scolon (Europe), in the directory /usr/spool/uucppublic/SSE. Note that access to these Supplements at scolon may not be available until December 2nd, 1994.

The filename conventions are as follows:

ssexxx.tar.Z - compressed tar file of supplement
ssexxx.ltr.Z - compressed cover letter for supplement

xxx indicates the number of the supplement, i.e. sse001.tar.Z.

See the README file in the directories listed above for checksum information. Connection information is available at the end of this document.

Please note that these Supplements are not generally available from SCO on diskette media.

If you have further questions, contact your support provider. If you need to contact SCO, please send electronic mail to support () sco COM, or contact SCO as follows.

USA/Canada: 6am-5pm Pacific Standard Time (PST)

1-800-347-4381 (voice)
1-408-427-5443 (fax)

Pacific Rim, Asia, and Latin American customers: 6am-5pm Pacific Standard Time (PST)

1-408-425-4726 (voice)
1-408-427-5443 (fax)

Europe, Middle East, Africa: 9am-5:30pm British Standard Time (BST)

+44 (0)923 816344 (voice)
+44 (0)923 817781 (fax)

Downloading Information
---

ftp to ftp.sco.com
Login name: ftp
Password: your email address

```
For anonymous UUCP connection:
------------------------------

For USA, Canada, Pacific Rim, Asia and Latin America customers:

Machine name:  sosco
Login name:  uusls  (fourth character is the letter "l")
No password

List of modems available for UUCP transfer from sosco.sco.com:

Standard V.32, (300-9600bps)     4@   408-425-3502
Hayes V Series 9600              2@   408-427-4470
Telebit Trailblazer                   408-429-1786


For Europe/Middle East/Africa customers there is a system located at
SCO EMEA (London):

Machine name:  scolon
Login name:  uusls
Password:  bbsuucp

List of modems available for UUCP transfer from scolon.sco.com:

Dowty Trailblazer  +44 (0)923 210911



For SCO Online Support (SOS) BBS download:
------------------------------------------

For those customers that have accounts on SOS these files can be
downloaded interactively via X, Y, Z MODEM or Kermit. Follow the
menus selections under "Toolchest" from the main SOS menu.

List of modems available for interactive transfer from sosco.sco.com:

First four are Standard V.32 (300-9600bps)      408-426-9495
Last three are Hayes 2400 compatible

Telebit Trailblazer                             408-426-9525



For ftp via World Wide Web:
---------------------------

URL to open:  ftp://www.sco.com

These problems, except for pt_chmod, were reported to the Santa Cruz
Operation by the "[8LGM] Security Team", 8lgm () bagpuss demon co uk.


--
-Christopher Durham                                  chrisdu () sco COM
Technical Support                                ...!uunet!sco!chrisdu
The Santa Cruz Operation
"...I think that when statesmen forsake their private conscience for the
sake of their public duties, they lead their country by a short route to
chaos."
        -Sir Thomas More to Cardinal Wolsey in _A Man for All Seasons_
```

--
Christopher William Klaus <cklaus () shadow net> <iss () shadow net>
Internet Security Systems, Inc.   Computer Security Consulting
2209 Summit Place Drive,   Penetration Analysis of Networks
Atlanta,GA 30350-2430. (404)518-0099. Fax: (404)518-0030

By Date By Thread

Current thread: