CERT Advisory CA-1993-08 SCO /bin/passwd Vulnerability

Original issue date: May 24, 1993
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center and the Santa Cruz Operation, Inc., (SCO) have recently identified a potential for compromising system integrity on several releases of SCO's Operating Systems. This potential will not allow unauthorized access to a system, but it may deny legitimate users the ability to log onto the system.

The releases of SCO product that are affected are as follows:

```
SCO UNIX System V/386 Release 3.2 Operating System Version 2.0
SCO UNIX System V/386 Release 3.2 Operating System Version 4.0
SCO UNIX System V/386 Release 3.2 Operating System Version 4.0 with
  Maintenance Supplement Version 4.1
SCO Open Desktop Release 1.1.x
SCO Open Desktop Release 2.0
```

Santa Cruz Operation and CERT recommend that sites using these SCO products take action to eliminate this vulnerability from their systems. This problem will be corrected in upcoming releases of SCO operating systems.

The Santa Cruz Operation has provided a Support Level Supplement (SLS), as described below. They have also provided an interim workaround until sites can obtain and install the Supplement.

If you have any questions about obtaining or installing the security supplement, contact SCO Support during normal business hours or send electronic mail to support@sco.com .

USA/Canada: 6am-5pm Pacific Daylight Time (PDT)

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

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

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)

I. Description

A problem exists in /bin/passwd in the SCO operating system versions detailed above.

II. Impact

This vulnerability can deny legitimate users the ability to log onto the system.

III. Solution

The Santa Cruz Operation and CERT recommend that all affected sites obtain and install the Support Level Supplement. Instructions are provided below.

The Santa Cruz Operation and CERT also recommend that sites consider applying the following workaround until they are able to obtain and install the Support Level Supplement.

1. Workaround

   This workaround will prevent users from changing their passwords until the Support Level Supplement is installed.

   As root, modify the permission on the existing /bin/passwd to prevent misuse.

   ```
   # /bin/chmod 2110 /bin/passwd
   ```

   Before installing the update, the permissions should again be reset. As root, modify the permission on the existing /bin/passwd.

```
# /bin/chmod 2111 /bin/passwd
```

1. Supplement

   SCO has prepared a Support Level Supplement (SLS) to address this issue. This is free to all customers, regardless of Support status. Sites can obtain this update via anonymous FTP from ftp.sco.COM (132.147.106.6). The files are located in:

```
Filename          File Contents              Size      Checksum
/SLS/uod368.Z     Update                   105857      62288
/SLS/uod368.ltr   ASCII Cover letter and     5514      29520
                  installation instructions
```

   The update may also be obtained from SCO via:

   - anonymous UUCP in the /usr/spool/uucppublic/SLS directory on the SOS bulletin board
   - CompuServe in the SCO Unix Library Section of the SCO Forum
   - hardcopy format (on diskette) from the media department at SCO Support.

   To retrieve and install the SCO Support Level Supplement, you must follow the instructions below. The detailed instructions described below will not be included in future advisories.

Beginning of Text provided by SCO

```
FTP download information:
=========================

You must have a connection to the Internet to use this service, and
should be familiar with the FTP command.

The command to use is:

ftp ftp.sco.COM

      or

ftp 132.147.106.6

You will be prompted for a login and password.  Log in as "anonymous" and
use your E-MAIL address as the password.

On ftp.sco.COM the fix and the cover letter files are in the ./SLS directory.
You will want to "cd" to this directory, set "binary", and "get" the files
uod368.Z and uod368.ltr.

Note that these files are also available from UUNET via anonymous FTP at
ftp.uu.net in the /sco-archive/SLS directory.

UUCP download information:
==========================

for the USA, Canadian, Pacific Rim, Asia, and Latin American customers:
- ------------------------------------------------------------------------
Machine name:   sosco
UUCP user:      uusls           (no password)
Modem Phone numbers:
Telebit Trailblazer Plus      408-429-1786      9600 baud
Telebit 1500 V.32, 2@         408-425-3502      2400, 9600 baud
Hayes V Series 9600, 2@       408-427-4470      9600 baud

for Europe, the Middle East, and Africa:
- ---------------------------------------
Machine name: scolon
UUCP user: uusls
Password: bbsuucp
Modem Phone numbers:
Dowty Trailblazer +44 (0)923 210911

The following information explains how to transfer the SLS from the
machine sosco using UUCP. A similar procedure can be used for scolon,
by changing the Systems file entry appropriately. This information assumes
that you are using an SCO Operating System to download the files. Other
systems may or may not be similar in their UUCP setup.

Before attempting to transfer, you must have a modem configured to dial out
from your computer.  For more information on configuring a modem, see the
chapter on "Adding Terminals and Modems" in the System Administrator's
Guide.
```

Once you have your modem configured for dialing out, you must set up
your UUCP configuration to recognize the SCO system which contains the
files. If you have a 2400 baud or lower speed modem, add the following
line to the end of the "Systems" configuration file in the directory
/usr/lib/uucp:

```
sosco Any ACU Any 14084253502 ogin:-@-ogin:-@-ogin: uusls

                              or

sosco Any ACU Any 14084274470 ogin:-@-ogin:-@-ogin: uusls
```

If you have a Telebit brand modem, use the following line:

```
sosco Any ACU Any 14084291786 ogin:-@-ogin:-@-ogin: uusls
```

Once your system is configured, you can use the uucp(C) command to
request files from the remote system. All files for Support Level
Supplements reside in /usr/spool/uucppublic/SLS.

The first file that should be downloaded is "uod368.Z" (the actual fix).
The uucp(C) command to transfer this file into the local directory
/usr/spool/uucppublic on your system would be:

```
uucp sosco!/usr/spool/uucppublic/SLS/uod368.Z /usr/spool/uucppublic/uod368.Z
```

(If you are using the C shell command interpreter, you must enter a
backslash character "\" before the exclamation mark "!" to prevent
the C shell history mechanism from intercepting the rest of the
command line.)

Next you would repeat the above procedure for "uod368.ltr" (the
cover letter for the fix).

Obtaining a hard copy of the SLS:
==========

This SLS is available in hard copy form. Customers should order it from their
Support provider or by calling SCO Support during normal business hours.
Please be sure to ask for "Support Level Supplement UOD368, the Security
Supplement". This is free to all customers, regardless of Support status.

```
        USA/Canada:
        -----------
        1-800-347-4381  (voice)
        1-408-427-5443  (fax)

        Pacific Rim, Asia, and Latin American customers:
        ------------------------------------------------
        1-408-425-4726  (voice)
        1-408-427-5443  (fax)

        Europe, Middle East, Africa:
        ----------------------------
        +44 (0)923 816344 (voice)
        +44 (0)923 817781 (fax)
```

Installation Preparation:
==========

1. Uncompress the file:

```
      uncompress uod368.Z
```

2. Format a diskette that is large enough to contain the file
   using the format(C) command.

3. Use the dd(C) command to transfer the file to diskette.

```
       dd if=uod368 of=/dev/fd0135ds18  for 3.5" diskettes or

       dd if=uod368 of=/dev/fd096ds15  for 5.25" diskettes
```

Follow the directions in the uod368.ltr file to install the Supplement.

End of Text provided by SCO

Revision History

September 19,1997 Attached Copyright Statement