CERT Advisory CA-1996-27 Vulnerability in HP Software Installation Programs

Original issue date: December 19, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The text of this advisory was originally released on October 11, 1996, as AA-96.04.Vulnerability.in.HP.Software.Installation.Programs, developed by AUSCERT. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AA-96.04
AUSCERT Advisory

Vulnerability in HP Software Installation Programs
11 October 1996

AUSCERT has received information that there is a vulnerability in the Hewlett Packard Software Distributor product, SD-UX, used to install, update, remove and package HP-UX software and patches. This software is installed by default under HP-UX 10.x and may have been specifically installed as additional software under HP-UX 9.x. Any system with the SD-UX package installed is vulnerable.

This vulnerability may allow local users to gain root privileges.

Exploit details involving this vulnerability have been made publicly available.

Vendor patches are being developed, but until they are made available, AUSCERT recommends that sites take the actions suggested in Section 3.

---

1. Description

The HP Software Distributor (SD-UX) is a package that provides a user interface which can be used to install, update, remove, and package HP-UX software and patches.

The programs supplied with this package create files in an insecure manner. As these programs execute with root privileges, it is possible to create or over-write arbitrary files on the system. The default location of the programs supplied by the package is /usr/sbin.

To determine if you have SD-UX installed on your system, check for the presence of the swinstall (and related) files using the following command:

```
% ls -l /usr/sbin/sw*
```

Individual sites are encouraged to check their systems for the SD-UX package, and if installed, take the actions recommended in Section 3.

2. Impact

Local users may be able to create or over-write arbitrary files on the system. This can be leveraged to gain root privileges.

3. Workarounds/Solution

AUSCERT recommends that sites prevent possible exploitation of this vulnerability by taking the measures stated in Section 3.1 immediately.

If software maintenance is required, AUSCERT advises that sites use one of the workarounds given in 3.2, preferably that described in Section 3.2.1.

Vendor patches may also address this vulnerability in the future (Section 3.3).

3.1 Remove permissions

Until official patches are available sites are encouraged to completely prevent the execution of all vulnerable SD-UX programs by any user (including root).

```
# chmod 400 /usr/sbin/swinstall
# chmod 400 /usr/sbin/swmodify
```

Note that if only the setuid permissions are removed, it is still possible for users to gain the privileges of any user executing the SD-UX programs (including root).

3.2 Workarounds

AUSCERT recommends that if software maintenance is required, sites implement one of the following workarounds until official vendor patches are made available.

The workaround described in 3.2.1 is the preferred method of doing software maintenance. If sites are unable to bring their machines into single user mode, the workaround given in Section 3.2.2 may be more applicable.

3.2.1 Run in single user mode

If packages must be installed, the machine should be brought into single-user mode, execute permissions re-enabled on /usr/sbin/swinstall,

```
# chmod 700 /usr/sbin/swinstall
# chmod 700 /usr/sbin/swmodify
```

and all symbolic links in /var/tmp and /tmp removed. The following command can be used to remove the symbolic links:

```
# find /tmp /var/tmp -type l -ok rm {} \;
```

Once this has been completed, any software package maintenance may be safely performed.

The execute permissions on the vulnerable programs must be removed before the machine is brought back into multi-user mode.

```
# chmod 400 /usr/sbin/swinstall
# chmod 400 /usr/sbin/swmodify
```

3.2.2 Change temporary file environment variable

This workaround should only be used if the SD-UX programs must be used while the machine is in multi-user mode.

The SD-UX programs use a number of temporary files. The location of these files can be configured using the environment variable TMPDIR. It is possible to set the environment variable TMPDIR to a non-world writable directory. Having the temporary files created in a non-world writable directory prevents the exploitation of the vulnerability described in this advisory.

NOTE: The environment variable must be set in each login session BEFORE any SD-UX programs are used.

To use this method, the following steps must be taken:

1. As root, create a non-world writable temporary directory for the temporary files used by the SD-UX programs. The location of these temporary files can be configured with the TMPDIR environment variable. In this workaround, we have chosen to use the directory /var/tmp/SD_tmp.

   ```
   # mkdir /var/tmp/SD_tmp
   # chmod 700 /var/tmp/SD_tmp
   ```

   For this workaround to be effective, sites should ensure that the parent directory of $TMPDIR has the sticky bit set if the parent directory is world writable. In this workaround, /var/tmp is the directory concerned. The sticky bit on /var/tmp can be set with the command:

   ```
   # chmod 1777 /var/tmp
   ```

   In all sessions where software maintenance is performed:
2. Change permissions on the vulnerable programs:

   ```
   # chmod 700 /usr/sbin/swinstall
   # chmod 700 /usr/sbin/swmodify
   ```
3. Set the environment variable TMPDIR:

   ```
   (under csh)
   # setenv TMPDIR /var/tmp/SD_tmp

   (under sh)
   # TMPDIR=/var/tmp/SD_tmp; export TMPDIR
   ```

   and verify that the directory exists and is writable by root.

   ```
   # ls -ld $TMPDIR
   ```
4. Perform any software package maintenance.
5. Remove the execute permissions on the vulnerable programs:

   ```
   # chmod 400 /usr/sbin/swinstall
   # chmod 400 /usr/sbin/swmodify
   ```
6. The environment variable TMPDIR is used by many other programs. You should either exit this interactive session, or reset the TMPDIR environment variables before continuing.

   NOTE: Steps 2) through 6) must be repeated each time software maintenance is performed.

3.3 Install vendor patches

Official vendor patches are currently being developed to address the vulnerability described in this advisory. When vendor patches are made available, AUSCERT suggests that they be installed.

AUSCERT thanks Information Technology Services of the University of Southern Queensland, Viviani Paz (The University of Queensland) and Hewlett Packard for their assistance in this matter.

UPDATES

Hewlett-Packard

Information concerning patches for the vulnerability described in this advisory can be found in HEWLETT-PACKARD SECURITY BULLETIN, "Security Vulnerability in swinstall command," Document ID: HPSBUX9707-064

1) From your Web browser, access the URL:

http://us-support.external.hp.com
(for US,Canada, Asia-Pacific, and Latin-America)

http://europe-support.external.hp.com
(for Europe)

2) On the HP Electronic Support Center main screen, select the hyperlink "Support Information Digests".

3) On the "Welcome to HP's Support Information Digests" screen, under the heading "Register Now", select the appropriate hyperlink "Americas and Asia-Pacific", or "Europe".

4) On the "New User Registration" screen, fill in the fields for the User Information and Password and then select the button labeled "Submit New User".

5) On the "User ID Assigned" screen, select the hyperlink "Support Information Digests".

Note what your assigned user ID and password are for future reference.

6) You should now be on the "HP Support Information Digests Main" screen. You might want to verify that your email address is correct as displayed on the screen. From this screen, you may also view/subscribe to the digests, including the security bulletins digest.

To get a patch matrix of current HP-UX and BLS security patches referenced by either Security Bulletin or Platform/OS, click on following screens in order:

Technical Knowledge Database
Browse Security Bulletins
Security Bulletins Archive
HP-UX Security Patch Matrix

Revision History

```
Sep. 24, 1997  Updated copyright statement
July 28, 1997 Updates section - added information from Hewlett-Packard.
```