CERT Advisory CA-1992-11 SunOS Environment Variables and setuid/setgid Vulnerability

Original issue date: May 27, 1992
Last revised: September 19, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability involving environment variables and setuid/setgid programs under Sun Microsystems Computer Corporation SunOS. This vulnerability exists on all Sun architectures running SunOS 4.0 and higher.

In-house and third-party software can also be impacted by this vulnerability. For example, the current versions of rnews, sudo, smount, and npasswd are known to be vulnerable under SunOS. See the Description section of this advisory for details of how to identify software which may be vulnerable.

The workaround detailed in this advisory can be used to protect vulnerable software on SunOS operating system versions for which patches are unavailable, or for local or third party software which may be vulnerable.

Sun has provided patches for SunOS 4.1, 4.1.1, and 4.1.2 programs which are known to be impacted by this vulnerability. They are available through your local Sun Answer Center as well as through anonymous ftp from the ftp.uu.net (137.39.1.9) system in the /systems/sun/sun-dist directory.

Fix	PatchID	Filename	Checksum
login and su	100630-01	100630-01.tar.Z	36269 39
sendmail	100377-04	100377-04.tar.Z	14692 311

Note: PatchID 100630-01 contains the international version of /usr/bin/login. PatchID 100631-01 contains the domestic version of /usr/bin/login and is only available from Sun Answer Centers for sites that use the US Encryption Kit.

Please note that Sun will occasionally update patch files. If you find that the checksum is different please contact Sun or the CERT/CC for verification.

I. Description

A security vulnerability exists if a set-user-id program changes its real and effective user ids to be the same (but not to the invoker's id), and subsequently causes a dynamically-linked program to be exec'd. A similar vulnerability exists for set-group-id programs.

In particular, SunOS /usr/lib/sendmail, /usr/bin/login, /usr/bin/su, and /usr/5bin/su are vulnerable to this problem.

II. Impact

Local users can gain unauthorized privileged access to the system.

III. Solution

A. Obtain and install the patches from Sun or from ftp.uu.net following the provided instructions.

B. The following workaround can be used to protect vulnerable binaries for which patches are unavailable for your SunOS version, or for local or third party software which may be vulnerable.

The example given is a workaround for /usr/lib/sendmail.

1. As root, rename the existing version of /usr/lib/sendmail and modify the permissions to prevent misuse.

```
# mv /usr/lib/sendmail /usr/lib/sendmail.dist
# chmod 755 /usr/lib/sendmail.dist
```

2. In an empty temporary directory, create a file wrapper.c containing the following C program source (remember to strip any leading white-space characters from the #define lines).

```
/* Start of C program source */

/* Change the next line to reflect the full pathname of the file to be protected by the wrapper code   */

            #define COMMAND "/usr/lib/sendmail.dist"
            #define VAR_NAME "LD_"

             main(argc,argv,envp)
             int argc;
             char **argv;
             char **envp;
             {
                     register char  **cpp;
                     register char  **xpp;
register char   *cp;

                     for (cpp = envp; cp = *cpp;) {
if (strncmp(cp, VAR_NAME, strlen(VAR_NAME))==0) {
for (xpp = cpp; xpp[0] = xpp[1]; xpp++);
                                        /* void */ ;
                             }
                             ee {

                                     cpp++;

                             }

}


                     execv(COMMAND, argv);

                     perror(COMMAND);

                     exit(1);

             }

/* End of C program source */
```

3. As root, compile the C program source for the wrapper and install the resulting binary.

```
# make wrapper
# mv ./wrapper /usr/lib/sendmail
# chown root /usr/lib/sendmail
# chmod 4711 /usr/lib/sendmail
```

4. Steps 1 through 3 should be repeated for other vulnerable programs with the appropriate substitution of pathnames and file names. The "COMMAND" C preprocessor variable within the C program source should also be changed to reflect the appropriate renamed system binary.

The CERT/CC wishes to thank the following for their assistance: CIAC, PCERT, and in particular Wietse Venema of Eindhoven University, The Netherlands, for his support in the analysis of and a workaround for this problem. We also wish to thank Sun Microsystems Computer Corporation for their prompt response to this vulnerability.

Revision History

```
September 19,1997  Attached copyright statement
```