CERT Advisory CA-1996-15 Vulnerability in Solaris 2.5 KCMS programs

Original issue date: July 31, 1996
Last revised: October 20, 1997
Vendor information for Sun has been added to the UPDATES section.

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

The text of this advisory was originally released on July 26, 1996, as AUSCERT Advisory AL-96.02, developed by the Australian Computer Emergency Response Team. 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.

Note that this vulnerability also affects Solaris 2.5.1.

The CERT/CC has received reports that this vulnerability has been exploited.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

AUSCERT have received a report of a vulnerability in the Sun Microsystems Solaris 2.5 distribution involving the programs kcms_calibrate and kcms_configure. These programs are part of the Kodak Color Management System (KCMS) packages.

This vulnerability may allow any local user to gain root privileges.

Exploit details involving this vulnerability have been made publicly available.

At this stage, AUSCERT is not aware of any official patches. AUSCERT recommends that sites take the actions suggested in Section 3 until official patches are available.

Depending on the local sites' requirements, the Solaris 2.5 KCMS packages may or may not have been installed. AUSCERT recommends that individual sites should determine whether the programs are installed and take appropriate action.

This Alert will be updated as more information becomes available.

---

1. Description

Solaris 2.5 contains support for the Kodak Color Management System (KCMS), a set of Openwindows compliant API's and libraries to create and manage profiles that can describe and control the colour performance of monitors, scanners, printers and film recorders.

KCMS includes the programs kcms_configure and kcms_calibrate which are used for the configuration and calibration of an X11 window system for use with the KCMS library. When installed, these programs have set-user-id root and set-group-id bin privileges.

A vulnerability involving these programs has been reported. Exploit details involving this vulnerability have been made publicly available.

Depending on the local sites' requirements, the Solaris 2.5 KCMS packages may or may not have been installed.

2. Impact

A local user may be able to create and then write to arbitrary files on the system. This can be leveraged to gain root privileges.

3. Workarounds/Solution

Currently, there are no official patches available. When patches are made available it is suggested the sites install the official

Until official patches are available sites are encouraged to remove the setuid and setgid permissions on the kcms_calibrate and kcms_configure programs. These are typically located in /usr/openwin/bin.

```
# chmod 400 /usr/openwin/bin/kcms_calibrate
# chmod 400 /usr/openwin/bin/kcms_configure
```

Note that this will remove the ability for users to run these programs.

AUSCERT wishes to thanks Marek Krawus of the University of Queensland for his assistance in this matter.

UPDATES

Vendor Information

Below is information we have received from vendors. If you do not see your vendor's name below, contact the vendor directly for information.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

103879-04 5.5.1
103881-04 5.5.1_x86
103878-04 5.5
103880-04 5.5_x86

Revision History

```
Oct. 20, 1997 Vendor information for Sun has been added to the UPDATES
              section
Sep. 24, 1997 Updated copyright statement
Feb. 25, 1997 Introduction - added information that CERT/CC has received
              reports of this vulnerability being exploited.
              Added copyright information.
Aug. 30, 1996 Information previously in the README was inserted into the
              advisory.
              Beginning of the AUSCERT text - removed AUSCERT advisory
              header to avoid confusion.
Aug. 02, 1996 Introduction - added information about Solaris 2.5.1.
```