

# [UNIX] Arbitrary File Corruption Vulnerability in Sun Solaris kcms\_configure

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0095.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 02/24/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 24 Feb 2005 17:49:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Arbitrary File Corruption Vulnerability in Sun Solaris kcms\_configure

---

## SUMMARY

The kcms\_configure utility is "part of the Kodak Color Management System (KCMS) package that is included with Solaris. It is installed setuid root by default".

Local exploitation of a race condition in the Kodak Color Management System's kcms\_configure script packaged with Sun Microsystems Inc. Solaris operating system can allow for the corruption of arbitrary files on the system.

## DETAILS

Vulnerable Systems:

\* Sun Solaris version 8, 9 (10 pre-release suspected)

Local exploitation of a race condition in the Kodak Color Management System's kcms\_configure script packaged with Sun Microsystems Inc. Solaris operating system can allow for the corruption of arbitrary files on the system.

## Securiteam: [UNIX] Arbitrary File Corruption Vulnerability in Sun Solaris kcms\_configure

The problem specifically exists due to logging errors within kcms\_configure, a set user id (setuid) root script. The file KCS\_ClogFile will be written to if it exists in the current directory. Due to a lack of sanity checking a local attacker can redirect log file output to an arbitrary file on the system through the usage of symbolic links. By specifying an invalid monitor profile argument the attacker can force an error log entry to be written.

Successful exploitation allows local attackers to corrupt arbitrary files on the system. Attackers can use this ability to append to important system files, possibly resulting in a denial of service or local privilege elevation.

### Workaround:

Remove the setuid bit from kcms\_configure:  
# chmod -s /usr/openwin/bin/kcms\_configure

### Vendor response:

This issue is addressed in Sun Alert  
<<http://www.sunsolve.sun.com/search/printfriendly.do?assetkey=1-26-57706-1>> ID #57706.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0481>>  
CAN-2004-0481

### Disclosure Timeline:

- \* 04/27/2004 – Initial vendor notification.
- \* 04/27/2004 – Initial vendor response.
- \* 02/23/2005 – Public disclosure.

## ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=206&type=vulnerabilities>>  
<http://www.idefense.com/application/poi/display?id=206&type=vulnerabilities>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,

Securiteam: [UNIX] Arbitrary File Corruption Vulnerability in Sun Solaris kcms\_configure  
loss of business profits or special damages.