CERT Advisory CA-1991-22 SunOS OpenWindows V3.0 Patch

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

=========================================================================
CA-91:22                        CERT Advisory
                              December 16, 1991
                        SunOS OpenWindows V3.0 Patch
- -------------------------------------------------------------------------
                      *** SUPERSEDED BY CA-93:18 ***

The Computer Emergency Response Team/Coordination Center (CERT/CC) has
received information concerning a vulnerability in Sun Microsystems,
Inc. (Sun) OpenWindows version 3.0.  This vulnerability exists on all
sun4 and sun4c architectures running SunOS 4.1.1.

Sun has provided a patch for this vulnerability.  It is available
through your local Sun Answer Center as well as through anonymous ftp
from the ftp.uu.net (192.48.96.2) system in the /sun-dist directory.

Fix                PatchID       Filename          Checksum
loadmodule         1076118       100448-01.tar.Z   04354  5

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

     An OpenWindows, version 3, setuid program (loadmodule(8)) can be
     exploited to execute a user's program using the effective UID of root.


II.  Impact

     This vulnerability allows a local user to gain root access.


III. Solution

     Obtain the patch from Sun or from ftp.uu.net and install, following the
     provided instructions.

     As root:

     1. Move the existing loadmodule aside.

        # mv $OPENWINHOME/bin/loadmodule $OPENWINHOME/bin/loadmodule.orig
        # chmod 400 $OPENWINHOME/bin/loadmodule.orig

     2. Copy the new loadmodule into the OpenWindows bin directory.

        # cp sun4/loadmodule $OPENWINHOME/bin/loadmodule
        # chown root $OPENWINHOME/bin/loadmodule
        # chmod 4755 $OPENWINHOME/bin/loadmodule

     See the README file provided with the patch for more information.
- -------------------------------------------------------------------------
The CERT/CC wishes to thank Ken Pon at Sun Microsystems, Inc. for alerting
us to this vulnerability.
- -------------------------------------------------------------------------

If you believe that your system has been compromised, contact CERT/CC via
telephone or e-mail.

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 24-hour hotline:
           CERT/CC personnel answer 7:30a.m.-6:00p.m. EST(GMT-5)/EDT(GMT-4),
           on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Past advisories and other information related to computer security are
available for anonymous ftp from the cert.org (192.88.209.5)
```

system.