CERT Advisory CA-1993-09a SunOS/Solaris /usr/lib /expreserve Vulnerability

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

- ---------------------------------------------------------------------------
CA-93:09a                      CERT Advisory
                               July 1, 1993
    REVISION NOTICE: SunOS/Solaris /usr/lib/expreserve Vulnerability
- ---------------------------------------------------------------------------
                 *** SUPERSEDED BY CA-96.19 ***
```

This REVISED CERT advisory contains Solaris patch information.

The CERT Coordination Center has received updated patch information concerning a vulnerability in /usr/lib/expreserve in Sun Microsystems, Inc. (Sun) operating system (SunOS). This vulnerability affects all sun3 and sun4 architectures and supported versions of SunOS including 4.1, 4.1.1, 4.1.2, 4.1.3, Solaris 2.0 (SunOS 5.0), Solaris 2.1 (SunOS 5.1), and Solaris 2.2 (SunOS 5.2). This problem has become widely known, and CERT recommends that sites take action to address this vulnerability as soon as possible.

Sun has produced a patch for SunOS 4.1, 4.1.1, 4.1.2, and 4.1.3 addressing this vulnerability for sun3 and sun4 architectures. Sun has also developed a patch for SunOS 5.x/Solaris 2.x systems. This revised advisory provides the information for obtaining the patch for SunOS 5.x/Solaris 2.x systems.

A workaround is provided below that can be used on all systems, including Solaris, until a patch is installed.

The patch can be obtained from local Sun Answer Centers worldwide as well as through anonymous FTP from the ftp.uu.net (192.48.96.9) system in the /systems/sun/sun-dist directory. In Europe, this patch is available from mcsun.eu.net (192.16.202.1) in the /sun/fixes directory.

System	Patch ID	Filename	BSD Checksum	Solaris Checksum
SunOS	101080-01	101080-01.tar.Z	45221 13	Not applicable
Solaris 2.0	101119-01	101119-01.tar.Z	47944 27	61863 54
Solaris 2.1	101089-01	101089-01.tar.Z	07227 27	4501 54
Solaris 2.2	101090-01	101090-01.tar.Z	02491 27	44985 54

The checksums shown above are from the BSD-based checksum (on Solaris, /usr/ucb/sum; on 4.x, /bin/sum) and from the SysV version that Sun released on Solaris (/usr/bin/sum). Please note that Sun sometimes updates patch files. If you find that the checksum is different please contact Sun or CERT for verification.

```
- ---------------------------------------------------------------------------
```

I.   Description

Expreserve is a utility that preserves the state of a file being edited by vi(1) or ex(1) when an edit session terminates abnormally or when the system crashes. A vulnerability exists that allows users to overwrite any file on the system.

II. Impact

It is possible to gain root privileges using this vulnerability.

III. Solution

A. Obtain and install the appropriate patch according to the instructions included with the patch.

B. Until you are able to install the appropriate patch, CERT recommends the following workaround be used on all systems. This workaround will disable expreserve functionality. The result of this workaround is that if vi(1) or ex(1) is running, and the sessions are interrupted, the files being edited will not be preserved and all edits not explicitly saved by the user will be lost. Users should be encouraged to save their files often.

As root, remove the execute permissions on the existing /usr/lib/expreserve program:

```
# /usr/bin/chmod  a-x  /usr/lib/expreserve
```

```
- -------------------------------------------------------------------------
```

The CERT Coordination Center wishes to thank Christopher Lott of Universitaet Kaiserslautern for reporting this vulnerability, and Sun Microsystems, Inc. for their response to this problem.

- ---

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in FIRST (Forum of Incident Response and Security Teams).

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
and are on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from cert.org (192.88.209.5).

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBOBS93Fr9kb5qlZHQEQIV/wCg8R25Cr6ELc1qfpzOOlvKmtKNE4EAoLMr
Jus2teX969Gvo6wdpSrkkcYU
=IFlI
-----END PGP SIGNATURE-----