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

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

- ---
CA-93:09 CERT Advisory
June 11, 1993
SunOS/Solaris /usr/lib/expreserve Vulnerability
- ---
*** SUPERSEDED BY CA-96.19 ***

The CERT Coordination Center has received 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 2.1 (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 is developing a patch for SunOS 5.x/Solaris 2.x systems and it will be released as soon as testing is complete. A workaround is provided below that can be used on all systems, including Solaris, until a patch is available and installed.

The patch can be obtained from local Sun Answer Centers worldwide as well as through anonymous FTP from the ftp.uu.net (137.39.1.9) 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.

Patch ID	Filename	Checksum
101080-1	101080-1.tar.Z	45221 13

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. If you are running SunOS 4.1, 4.1.1, 4.1.2, or 4.1.3, obtain and install the patch according to the instructions included with the patch.

B. If you are running Solaris install the following workaround. 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/AwUBOBS91Vr9kb5qlZHQEQLSKQCfeRgPlsyzOmBx7X+7rDgjs3tl3xwAnjVR
fXxUbNt6+0jnqQmDyJNb97eX
=QCZG
-----END PGP SIGNATURE-----