CERT Advisory CA-1991-10 REVISION NOTICE: New Patch for SunOS /usr/lib/lpd

Original issue date: September 12, 1991
Last revised: September 18, 1997
Attached copyright statement

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

***** THIS IS A REVISED CERT ADVISORY *****
***** CONTAINS NEW INFORMATION *****

There were a number of problems with various early versions of Sun Microsystems, Inc. (Sun) /usr/lib/lpd patch (Patch ID 100305-xx). While security problems were fixed in the patches, a remote print spooling problem was introduced. Sun believes all the problems have been fixed and they are now releasing the enclosed information concerning a new patch version. They have given the CERT/CC permission to distribute this information.

The Computer Emergency Response Team/Coordination Center (CERT/CC) recommends that all affected sites follow the information provided by Sun Microsystems in this bulletin.

START OF SUN-SUPPLIED INFORMATION

SUN MICROSYSTEMS SECURITY BULLETIN:

This information is only to be used for the purpose of alerting customers to problems. Any other use or re-broadcast of this information without the express written consent of Sun Microsystems shall be prohibited.

Sun expressly disclaims all liability for any misuse of this information by any third party.

This is more an update on the lpd fix than any new information.

First the update.

After a lengthy beta test cycle, there is now available a new version of the lpd security fix. The patch-ID# is 100305-06.

This patch is available via anonymous ftp from the ftp.uu.net system in the sun-dist directory as 100305-06.tar.Z, or through your local Sun Answer Center. The checksum information for the file available from ftp.uu.net is:

```
24474   440   100305-06.tar.Z
```

Some history.

An lpd bug was discovered where lpd could be used to remove system files (/etc/passwd or /.rhosts as examples). This bug was fixed with 100305-01.

A second bug was also shown that could still be used to remove system files. This fix was rolled into 100305-02.

An lpc problem that touched one of the same modules as in the lpd fix was fixed and the subsequent change rolled into the lpd patch 100305-03.

Two additional problems were sent to Sun: one having to do with RPC calls to lpd and the second having to do with postscript calls to lpd, thus 100305-04.

It was in creating the -04 version that we unknowingly introduced a remote spool problem on the SunOS 4.1.1 version of the patch. The problem was that if the remote queue had jobs in it, the local job sent was often truncated to zero length.

The -05 version was an attempt to back out the last few changes to remove the remote print problem. Unfortunately, it did not. It was at this time that we decided to do a lengthy evaluation and test cycle to ensure that the newest version fixed all the reported problems as well as fixed the remote spool bug we had introduced.

The 100305-06 patch is the result of that lengthy test cycle.

Thank you all for your support through all this.

Brad Powell
Software Security Coordinator
Sun Microsystems.

END OF SUN-SUPPLIED INFORMATION

Revision History

```
September 18,1997  Attached copyright statement
```