CERT Advisory CA-1993-19 Solaris System Startup Vulnerability

Original issue date: December 16, 1993
Last revised: September 19, 1997
Added Sun patch information.
Attached copyright statement

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

The CERT Coordination Center has received information concerning a vulnerability in the system startup scripts on Solaris 2.x and Solaris x86 systems. The changes described below will be integrated into the upcoming Solaris release.

I. Description

If *fsck(8)* fails during system boot, a privileged shell is run on the system console. This behavior can represent a security vulnerability if users, who would normally not have root access, have physical access to the console at boot time. An attacker can force the failure to occur.

II. Impact

This vulnerability allows anyone with physical access to the system console to gain root access.

III. Solution

A simple change to each of two system scripts can be used to close this potential security hole. The new behavior will cause the system to run the privileged shell only if the user at the console enters the correct root password.

If you wish to make the change on your own systems, edit both /sbin/rcS and /sbin/mountall, changing every occurrence of:

```
/sbin/sh < /dev/console
```

to:

```
/sbin/sulogin < /dev/console
```

As distributed by Sun, /sbin/rcS contains one occurrence of this string, at line 152; and /sbin/mountall contains two, one at line 66 and one at line 250.

Once these changes are made, sulogin will request the root password in the event *fsck(8)* fails, before starting a privileged shell. The success or failure of sulogin will be logged in /var/adm/sulog.

The CERT Coordination Center wishes to thank Sun Microsystems, Inc. for their support in responding to this problem.

UPDATES

September 19, 1997:

BUG 1124898 is fixed in Solaris 2.4

Revision History

```
Sept 19, 1997  Updates - Added Sun patch information.
               Attached copyright statement
```