CERT Advisory CA-1990-12 SunOS TIOCCONS Vulnerability

Original issue date: December 20, 1990
Last revised: September 17, 1997
Attached copyright statement

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

The following information was sent to us from Sun Microsystems. It contains availability information regarding a fix for a vulnerability in SunOS 4.1 and SunOS 4.1.1. (A version for SunOS 4.0.3 is currently in testing and should be available shortly.) For more information, please contact Sun Microsystems at 1-800-USA-4SUN.

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.

These patches are available through your local Sun answer centers worldwide. As well as through anonymous ftp to ftp.uu.net:~ftp/sun-dist

```
sum of SunOS 4.1 tarfile 100187-01.tar.Z  : 14138   142
sum of SunOS 4.1.1 tarfile 100188-01.tar.Z: 24122   111
```

README information follows:

Patch-ID# 100188-01
Keywords: TIOCCONS
Synopsis: SunOS 4.1.1: TIOCCONS redirection of console is a security violation.
Date: 17/Dec/90

SunOS release: 4.1.1

Unbundled Product:

Unbundled Release:

Topic:

BugId's fixed with this patch: 1008324

Architectures for which this patch is available: sun3 sun3x sun4 sun4c

Patches which may conflict with this patch:

Obsoleted by: Next major release of SunOS

Problem Description: TIOCCONS can be used to re-direct console output/input away from "console"

Patch contains kernel object modules for:

```
/sys/sun?/OBJ/cons.o
/sys/sun?/OBJ/zs_async.o
/sys/sun?/OBJ/mcp_async.o
/sys/sun?/OBJ/mti.o
```

Where sun? is one of sun4, sun4c, sun3, sun3x, sun4/490-4.1_PSR_A

NOTE: The sun4c does not use mti.o nor mcp_async.o since this architecture does not have VME slots and therefore cannot use the ALM-2 Asynchronous Line Multiplexor or Systech MTI-800/1600. So those modules are not needed.

The fix consists of adding permission checking to setcons, the routine that does the work of console redirection, and changing its callers to supply additional information required for the check and to see whether or not the check succeeded. Setcons now uses uid and gid information supplied to it as new arguments to perform a VOP_ACCESS call for VREAD permission on the console. If the caller doesn't have permission to read from the console, setcons rejects the redirection attempt.

Install

As Root:

save aside the object modules from the FCS tapes as a precaution:

```
# mv /sys/sun?/OBJ/cons.o /sys/sun?/OBJ/cons.o.orig
# mv /sys/sun?/OBJ/tty_pty.o /sys/sun?/OBJ/tty_pty.o.orig
# mv /sys/sun?/OBJ/zs_async.o /sys/sun?/OBJ/zs_async.o.orig
# mv /sys/sun?/OBJ/mcp_async.o /sys/sun?/OBJ/mcp_async.o.orig
# mv /sys/sun?/OBJ/mti.o /sys/sun?/OBJ/mti.o.orig
```

copy the new ".o" files to the OBJ directory:

```
# cp sun?/*.o /sys/sun?/OBJ/
```

build and install a new kernel:

```
rerun /etc/config  and do a "make" for the new kernel
```

Please refer to the System and Network Administration Manual for details on how to configure and install a custom kernel.

Patch-ID# 100187-01
Keywords: TIOCCONS
Synopsis: SunOS 4.1 4.1_PSR_A: TIOCCONS redirection of console is a security violation.
Date: 17/Dec/90

SunOS release: 4.1 4.1_PSR_A

Unbundled Product:

Unbundled Release:

Topic:

BugId's fixed with this patch: 1008324

Architectures for which this patch is available: sun3 sun3x sun4 sun4c sun4-490_4.1_PSR_A

Patches which may conflict with this patch:

Obsoleted by: Next major release of SunOS

Problem Description

TIOCCONS can be used to re-direct console output/input away from "console"

Patch contains kernel object modules for:

```
/sys/sun?/OBJ/cons.o
/sys/sun?/OBJ/zs_async.o
/sys/sun?/OBJ/mcp_async.o
/sys/sun?/OBJ/mti.o
```

Where sun? is one of sun4, sun4c, sun3, sun3x, sun4/490-4.1_PSR_ABR

NOTE: The sun4c does not use mti.o nor mcp_async.o since this architecture does not have VME slots and therefore cannot use the ALM-2 Asynchronous Line Multiplexed or Systech MTI-800/1600. So those modules are not needed.

The fix consists of adding permission checking to setcons, the routine that does the work of console redirection, and changing its callers to supply additional information required for the check and to see whether or not the check succeeded. Setcons now uses uid and gid information supplied to it as new arguments to perform a VOP_ACCESS call for VREAD permission on the console. If the caller doesn't have permission to read from the console, setcons rejects the redirection attempt.

Install

As Root:

Save aside the object modules from the FCS tapes as a precaution:

```
# mv /sys/sun?/OBJ/cons.o /sys/sun?/OBJ/cons.o.orig
# mv /sys/sun?/OBJ/tty_pty.o /sys/sun?/OBJ/tty_pty.o.orig
# mv /sys/sun?/OBJ/zs_async.o /sys/sun?/OBJ/zs_async.o.orig
# mv /sys/sun?/OBJ/mcp_async.o /sys/sun?/OBJ/mcp_async.o.orig
# mv /sys/sun?/OBJ/mti.o /sys/sun?/OBJ/mti.o.orig
```

copy the new ".o" files to the OBJ directory:

```
# cp sun?/*.o /sys/sun?/OBJ/
```

Build and install a new kernel: rerun /etc/config and do a "make" for the new kernel

Please refer to the System and Network Administration Manual for details on how to configure and install a custom kernel.

Revision History

```
September 17, 1997  Attacced copyright statement
```