



Trusted Solaris 8 4/01 Release Notes

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part No: 816-1043-10
November 2001

Copyright 2001 Sun Microsystems, Inc. 901 San Antonio Road Palo Alto, CA 94303-4900 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, Solaris Management Console, SunScreen, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2001 Sun Microsystems, Inc. 901 San Antonio Road Palo Alto, CA 94303-4900 U.S.A. Tous droits réservés

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, Solaris Management Console, SunScreen, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPOUDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



011210 @2870



Contents

1	Trusted Solaris 8 4/01 Release Notes	5
	Getting Help	6
	Reading About the Changes and Features in the Trusted Solaris 8 4/01 Release	6
	Ordering Sun Documents	6
	Supported Hardware	7
	Solaris Bug Fixes Incorporated in This Release	7
	Trusted Solaris 8 Bugs Fixed in This Release	9
	Known Problems With the Software	9
	Languages CD is not supported	9
	praudit and auditreduce do not work with RBAC profile entries (4508276)	10
	Communication between TSIX host types with IPsec AH is broken (4471447)	10
	IKE does not work with the TSOL host type (4548783)	10
	nisaddent causes a SIGSEGV error when adding to tnrrhdb (4491941)	10
	Some suser () calls still exist in kernel (4493976)	11
	File system label ranges are not enforced for unlabeled NFS file systems (4150441)	11
	Graphical Window Manager controls do not work (4462771)	12
	niscat command hangs and spawns multiple nisd processes on a NIS+ server (4430740)	12
	Trusted Solaris label encodings file requires coding for ILs (4329208)	12
	The smosservice command fails to create OS server (4378498)	13
	Device Allocation: Configuration dialog box does not configure the first device (4533649)	13
	Drag and drop does not work for OpenLook applications (4095021)	13

Nonexistent location ID: FileManagerLabelsHelp (4477399) 13

SMC Mounts and Shares tools do not set or modify Trusted Solaris attributes
(4496897) 14

Trusted Solaris 8 4/01 Release Notes

Note – We strongly recommend that you read and use *Trusted Solaris Installation and Configuration* (PN 816–1040–10) to guide you in configuring the Trusted Solaris operating environment. The differences between this secure operating environment and a Solaris operating environment, such as – labels, clearance confirmations, obligatory passwords, security configuration choices, name service domain setup, secure network setup, and no superuser – require planning and guidance during installation and configuration.

The Trusted Solaris 8 4/01 operating environment upgrades the Trusted Solaris 8 release and enhances the following software with security: Solaris 8 4/01 operating environment, CDE 1.4.4 (Common Desktop Environment), and the Solaris Management Console 2.0 administrative interface. The release incorporates patches to the Trusted Solaris 8 operating environment, the window system, and patches for the Solaris, CDE and Solaris Management Console releases. In particular, this release incorporates many security bug fixes.



Caution – Do not apply patches that may be available for the standard releases of Solaris software, CDE, X Windows, or Solaris Management Console.

The sections are as follows:

- “Getting Help” on page 6
- “Supported Hardware” on page 7
- “Solaris Bug Fixes Incorporated in This Release” on page 7
- “Trusted Solaris 8 Bugs Fixed in This Release” on page 9
- “Known Problems With the Software” on page 9

Getting Help

For assistance in using the document set, see the *Trusted Solaris Roadmap* (PN 816-1039-10) document.

The docs.sun.comSM web site enables you to access Sun technical documentation online. You can browse the <http://docs.sun.com> archive or search there for a specific book title or subject.

Reading About the Changes and Features in the Trusted Solaris 8 4/01 Release

Read the following for specific information.

Trusted Solaris 8 Release Notes

For bugs fixed between the Trusted Solaris 7 and Trusted Solaris 8 releases.

Trusted Solaris 8 4/01 Transition Guide

For changes from the Trusted Solaris 8 and Trusted Solaris 7 releases to the current release.

Solaris 8 4/01 What's New

For features that the Trusted Solaris 8 4/01 release inherits from the Solaris 8 release.

Solaris 8 (SPARC Platform Edition) 4/01 Release Notes Update

For information about the Solaris 8 4/01 release.

Solaris 8 (Intel Platform Edition) 4/01 Release Notes Update

For information about the Solaris 8 4/01 release.

Ordering Sun Documents

Fatbrain.com, the Internet's most comprehensive professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at <http://www1.fatbrain.com/documentation/sun>.

Supported Hardware

The Trusted Solaris 8 4/01 release supports the workstation, server, and peripherals hardware supported by the Solaris 8 4/01 release. See also:

- *Solaris 8 4/01 Sun Hardware Platform Guide* in the *Solaris 8 4/01 on Sun Hardware Collection*
- *Solaris 8 (Intel Platform Edition) 4/01 Hardware Compatibility List*

Solaris Bug Fixes Incorporated in This Release

The Trusted Solaris 8 4/01 release includes all product patches and bug fixes incorporated into the Solaris 8 4/01 release. The bug fixes that are listed in the tables below are additional.

Security bugs that are fixed in releases later than Solaris 8 4/01 have been incorporated into this release. The Trusted Solaris 8 4/01 release includes the following Solaris security bug fixes:

TABLE 1–1 Solaris Security Bug Fixes Integrated in Trusted Solaris 8 4/01

Solaris Bug Number	Synopsis
4153434, 4274696	\$TZ environment variable not totally safe
4328124	Security hole in <code>rmmount.conf</code> - possible string buffer overflow
4330421, 4383387	LP subsystem is vulnerable to printing unauthorized files
4338622	Buffer overflow vulnerabilities in Kerberos (SEAM)
4356377, 4425845, 4440161	Buffer overflow vulnerabilities in keyboard DDX module
4392144, 4434978	<code>catman</code> makes dangerous use of <code>tmpfiles</code>
4406722	Buffer overflow in <code>cu(1C)</code> allows access as <code>uucp</code> UID
4409676, 4444745	CERT Advisory CA-2001-02 / Solaris DNS (BIND) vulnerabilities
4412996, 4451002	Buffer overflow in <code>snmpXdmid</code> allows remote root compromise

TABLE 1-1 Solaris Security Bug Fixes Integrated in Trusted Solaris 8 4/01 (Continued)

Solaris Bug Number	Synopsis
4414237	snmpXdmi has hard-coded security strings
4416701	Buffer overflow in uucp can allow access as uucp UID
4430971	tip, getent () can ignore supplied buffer size
4432295	send () with a negative "len" arg puts kernel in a loop - DOS attack
4436988	CERT CA-2001-07 / Globbing problem in in.ftpd
4439142	Kernel preemption can corrupt floating point register
4448598	Buffer overflow in LANG dtsession variable
4449613	Buffer overflow in libsldap.so.1 compromises root
4450699	Solaris Intel system can panic from user process
4451291	CDE: Buffer overflow in libXm.so.4
4456994	Buffer overflow in rpc.yppasswdd
4465086	Buffer overflow in /bin/mail
4477380	Buffer overflow in /usr/bin/whodo via \$TZ
4370975, 4414939	CDE: Motif text widget accesses illegal memory addresses
4411170	CDE: dtfile dumps core at draw_separator () when resizing window
4446925, 4458432	in.lpd contains a remote exploitable overflow
4448655	telmod.c could panic the system
4452732	Buffer overflow in mailx
4466215, 4482260	ckitem(1) could cause stack overflow
4499995	Format string vulnerability in ToolTalk Database Server

TABLE 1-2 Solaris Bug Fixes Integrated in Trusted Solaris 8 4/01

Solaris Bug Number	Synopsis
4418312	turnstile_block () does not accurately detect cycle in blocking chain
4300800	inet_ntop (): BAD TRAP: type=e (Page Fault) rp=ef4229d8 addr=e0f1007

Trusted Solaris 8 Bugs Fixed in This Release

The following bugs reported in the *Trusted Solaris 8 Release Notes* have been fixed in the Trusted Solaris 8 4/01 software:

- (4256066) `bind()` and `accept()` do not generate audit records
- (4388344) The `/etc/shadow` file can be relabeled
- (4384632) Label daemon is not locale-aware
- (4490513) Cannot modify label range of attached printer using Device Allocation Manager
- (4384781) NIS (YP) account cannot see assigned profiles
- (4380852) SMC returns error for a valid IPv6 address
- (4385223) SMC Scheduled Jobs tool supports `admin_low` jobs only
- (4381198) Switching between scopes in SMC is not robust
- (4291482) The TSIX network protocol does not work
- (4385479) CDE exit sometimes fails
- (4284167) The `swmtool` utility does not work
- (4358479, 4357512) SMC auditing is incomplete

Known Problems With the Software

This section identifies known problems in the Trusted Solaris 8 4/01 software, describes them, and suggests solutions to them. These bugs may or may not be fixed in a future release.

Languages CD is not supported

This release supports only the C locale (U.S. English). Thus, no Languages CD is provided.

praudit and auditreduce do not work with RBAC profile entries (4508276)

The praudit and auditreduce commands are both listed in the Audit Review profile as requiring `euid=0`. This should work, but in fact `uid=0` is required.

Workaround: Change the two entries in the `exec_attr` database to use `uid=0` instead of `euid=0`.

Communication between TSIX host types with IPsec AH is broken (4471447)

Network packets using the TSIX protocol are not processed correctly when AH headers are present.

Workaround: None.

IKE does not work with the TSOL host type (4548783)

Network packets that are labeled with the TSOL protocol are not processed correctly by IKE in the SunScreen™ 3.2 product that is co-packaged with this release. The SunScreen log messages show `IKE_INVALID_COOKIE`.

SunScreen properly processes TSOL-labeled network traffic that is in clear text. SunScreen IKE also behaves correctly in the Trusted Solaris operating environment to protect traffic between unlabeled network connections.

Workaround: None.

nisaddent causes a SIGSEGV error when adding to tnrhdb (4491941)

A `SIGSEGV` error is produced when using the `nisaddent -avf` command to add an incorrectly formatted file to the `tnrhdb` NIS+ map. This produces a core dump.

Workaround: The `nisaddent` command works correctly with a valid input file. To ensure that the input file has fields separated by colons and not by spaces, use `niscat -s :` when dumping a NIS+ table that will be used later as input to NIS+.

Some `suser()` calls still exist in kernel (4493976)

The interfaces listed below have code paths which check for the `sys_suser_compat` privilege instead of the proper privilege.

- `LOG_FLUSH`, `SVCPOOL_CREATE` opcodes for `NFSSYS()`.
- Creation/deletion of a ufs file system snapshot via the `_FIOSNAPSHOTCREATE` and `_FIOSNAPSHOTDELETE` ioctl commands.
- Many of the power-management ioctls. These are nominally used by `/usr/sbin/pmconfig`, and include the following ioctls:
 - `PM_SET_THRESHOLD`
 - `PM_SET_CUR_PWRPM_ADD_DEP`
 - `PM_REM_DEVICES`
 - `PM_SET_DEVICE_THRESHOLD`
 - `PM_SET_SYSTEM_THRESHOLD`
 - `PM_START_PM`
 - `PM_STOP_PM`
 - `PM_RESET_PM`
 - `PM_DIRECT_PM`
 - `PM_RESET_DEVICE_THRESHOLD`
 - `PM_SET_COMPONENT_THRESHOLDS`
 - `PM_IDLE_DOWN`
 - `PM_ADD_DEPENDENT`
 - `PM_ADD_DEPENDENT_PROPERTY`
- The `PPMIOCSET` ioctl for power management.

Workaround: These interfaces may need to be invoked with the `PRIV_SUSER_COMPAT` privilege. This can be accomplished via profiles by using an `exec_attr` entry specifying this privilege.

File system label ranges are not enforced for unlabeled NFS file systems (4150441)

This bug occurs in a very unusual situation. The administrator must have consciously configured a NFS remote host to be at one label, and the label range to be another.

Workaround: To prevent the creation of files at the default label for the server, mount the file system as "read-only". Existing files are unaffected, but the read-only mount option prevents the creation of files at a label outside the label range.

Graphical Window Manager controls do not work (4462771)

The new utilities `sdtgwm`, `sdtwsm`, and `sdtwinlst` and their corresponding actions in the `Desktop_Apps` folder generate errors, such as `Warning: Query Module Not Running`.

Workaround: None. These tools are inappropriate for users in the Trusted Solaris environment. They are not supported.

`niscat` command hangs and spawns multiple `nisd` processes on a NIS+ server (4430740)

The bug is known to occur when SMC is running on a NIS+ client or master and has loaded its toolbox from a NIS+ replica. Next, the replica is shut down and SMC is used to update any NIS+ maps. Since the machine from which SMC loaded its toolbox is down, the SMC client has no way to communicate with the SMC server, which is the machine from which the toolbox has been loaded.

Workaround: Do not use SMC to update NIS+ databases when a NIS+ replica is down. Use the standard NIS+ command line interface instead.

Trusted Solaris label encodings file requires coding for ILs (4329208)

Although Trusted Solaris 8 4/01 software does not support information labels (ILs), the `chk_encodings(1M)` command fails with the following error if the `label_encodings` file omits information about ILs.

```
# chk_encodings label_encodings
Label encodings conversion error at line 37:
  Can't find INFORMATION LABELS specification.
  Found instead: "SENSITIVITY LABELS:".
label_encodings: label encodings syntax check failed.
```

Workaround: Copy a valid `SENSITIVITY LABELS:` section in your `label_encodings` file, and rename it to `INFORMATION LABELS:`, as in:

```
INFORMATION LABELS:
...
WORDS:
...
REQUIRED COMBINATIONS:
...
```

COMBINATION CONSTRAINTS:

...

The smosservice command fails to create OS server (4378498)

The SMC commands `smosservice` and `smdiskless` do not work correctly.

Workaround: Set up diskless service manually. On the OS server, name and allocate the client disk partitions during the installation program.

Device Allocation: Configuration dialog box does not configure the first device (4533649)

A device's configuration is unchanged the first time that you click OK in the Device Allocation: Configuration dialog box.

Workaround: Repeat the configuration procedure without closing the Device Allocation Manager. When you have repeated the procedure, you can then configure other devices without clicking OK a second time.

Drag and drop does not work for OpenLook applications (4095021)

Drag and drop operations do not work reliably for OpenLook applications.

Workaround: Use the copy and paste keys with OpenLook applications.

Nonexistent location ID: FileManagerLabelsHelp (4477399)

This bug is seen when you perform the following steps:

1. Insert Floppy disk.
floppy_0 is allocated by Device Allocation Manager.
2. From File Manager, click the File menu and select Removable Media Manager.
3. Select the floppy icon and click mouse button 3 to open the Labels menu item.

4. In Removable Media Manager - File Labels (the Trusted Solaris Label Builder), click the Help button at bottom right of the dialog box.

Workaround: Perform the following steps:

1. Click mouse button 3 on the Front Panel and select Help from the pop-up menu. The Workspace Manager – Help window appears.
2. In the Workspace Manager – Help window, scroll down in the top pane to Trusted Solaris Applications and select it.
3. In the bottom pane, click Create Labels.

SMC Mounts and Shares tools do not set or modify Trusted Solaris attributes (4496897)

The SMC Mounts tool and SMC Shares tool do not manipulate Trusted Solaris attributes.

Workaround: Use the Set Mount Points and Share Filesystems actions to handle Trusted Solaris attributes, or use the Admin Editor on the `/etc/vfstab` and the `/etc/dfs/dfstab` file.