UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA MAINTENANCE REPORT MR1 (supplementing Certification Report No. P170)

Sun Microsystems, Inc. Trusted Solaris ™

Version 8 2/04

Issue 1.0

March 2006

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the addendum to the original Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the addendum has been issued in accordance with the terms of this Arrangement.

The judgements contained in this report are those of the Qualified Certification Body which issued it. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

TABLE OF CONTENTS

Abbreviations

CCRA	Common Criteria Recognition Arrangement
CDE	Common Desktop Environment
EAL	Evaluation Assurance Level
IAR	Impact Analysis Report
OBP	OpenBoot PROM
OBPSC	OpenBoot PROM System Controller
SC	System Controller
SF	Security Function
SFR	Security Functional Requirement
SMC	Solaris Management Console
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSOL	Trusted Solaris

References

a. Common Criteria Certification Report No. P170, Sun Microsystems Inc.,
Trusted Solaris Version 8 4/01,
UK IT Security Evaluation and Certification Scheme,
Issue 3.0, March 2004.

b. Trusted Solaris 8 4/01 Security Target,
Sun Microsystems Inc.,
TS8_101, Issue 3.1, 12 November 2003.

c. Trusted Solaris 8 2/04 Security Target
Sun Microsystems Inc.,
TS8_101, Issue 1.1, 20 February 2006

d. Arrangement on the Recognition of Common Criteria Certificates in the Field of
Information Technology Security,
Members of the Agreement Group,
May 2000.

e. Assurance Continuity: CCRA Requirements,
Common Criteria Interpretation Management Board,
CCIMB-2004-02-09, Version 1.0, February 2004.

f. Trusted Solaris 8 2/04 Impact Analysis Roadmap
Issue 1.0, 30 October 2005

g. Trusted Solaris 8 2/04 Security Impact Analysis
Issue 1.0, June 2005

h. Trusted Solaris 8 HW 7/03 Security Impact Analysis
Issue 1.0, November 2003

i. Trusted Solaris 8 HW 12/02 Security Impact Analysis
Issue 1.0, July 2003

Introduction

1. This Maintenance Report outlines the current status of the Assurance Continuity process for versions of Trusted Solaris 8, and is intended to assist prospective consumers when judging the suitability of the IT security of the versions of the product for their particular requirements.

2. The baseline for assurance maintenance was the Common Criteria evaluation, to the EAL4 Evaluation Assurance Level, augmented by ALC_FLR.3, of Trusted Solaris 8 4/01.

3. Prospective consumers are advised to read this document in conjunction with:

- the Certification Report [Reference a] for the evaluation of the original certified Target of Evaluation (TOE), to which this report is an addendum;
- the Security Target [b] of the certified TOE, which specifies the functional, environmental and assurance requirements for the evaluation; and
- the updated Security Target [c] of the maintained derivative.

Maintained Versions

4. The version of the product originally evaluated was:

- Trusted Solaris 8 4/01.

5. The version of the product for which assurance has subsequently been maintained is:

- Trusted Solaris 8 2/04.

6. Note that for the maintained version the scope of TOE functionality remains unchanged from that of the certified version, as defined in the respective Security Targets [b, c], although there have been some minor changes and bugfixes to the product and different hardware platforms are used.

Assurance Continuity Process

7. The Common Criteria Recognition Arrangement (CCRA) [d] has been established as a basis for the mutual recognition of the results of Common Criteria evaluations. The process of Assurance Continuity within Common Criteria is defined in the document 'Assurance Continuity: CCRA Requirements' [e].

8. The Assurance Continuity process is based on an Impact Analysis Report (IAR), produced by the Developer, which describes all the changes made to the product, and assesses the security impact of each change. The Trusted Solaris 8 2/04 IAR [f] is supported by Security Impact Analyses [g, h, i] for each of the Trusted Solaris 8 versions HW 12/02, HW 7/03 and 2/04. These documents have been examined by the UK IT

Security Evaluation and Certification Scheme, Certification Body, who produced this Maintenance Report.

9. The Developer, Sun, has carried out full retesting on Trusted Solaris 8 2/04 and has considered all the assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [e].

10. The Certification Body accepts the decisions detailed in the IAR [f], which has assessed each change as being of ***minor*** impact, and concludes that the overall impact of all the changes is ***minor***.

11. After consideration of the IAR [f] and other visibility of the assurance continuity process given to the Certifier, the Certification Body has determined that EAL4 assurance, augmented by ALC_FLR.3, has been maintained for the derived version, Trusted Solaris 8 2/04.

General Points

12. Assurance continuity addresses the security functionality claimed in the Security Target [c] with reference to the assumed environment specified. The assurance maintained configurations are as specified by the modifications specified in this report in conjunction with the original Certification Report [a]. Prospective consumers are advised to check that this matches their identified requirements.

13. The assurance continuity process is not a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the assurance continuity process has been completed. Existing and prospective consumers should check for themselves whether any security vulnerabilities have been discovered since this report and, if appropriate, should check with the vendor to see if any patches exist for the product.

Analysis of Changes

14. There are no new TOE Security Policy (TSP) enforcing components in Trusted Solaris 8 2/04. There are no changes to the high-level design, and changes to TSP enforcing code are limited to the removal of vulnerabilities and other coding errors.

15. The IAR [f], in analysing code changes, distinguishes between TSP-critical code (code that directly implements one or more Security Functional Requirements (SFRs)) and TSP-supporting code (all other code within the ‘TOE Security Functions’ (TSF)). Changes between Trusted Solaris 8 4/01 and the 2/04 version fall into one of the following categories.

- Changes to TSP-critical code.
- Changes to TSP-supporting code to remove actual or potential vulnerabilities.

- Changes to TSP-supporting code that are relevant to security, e.g. improving usability of security functions, or tightening security policy controls beyond those specified in the Security Target [c].

- Man page changes.

- Changes to user profiles or command privileges

- Changes to installation scripts (these include some fixes to maintenance environment bugs).

- Changes that have no relevance to security.

Additionally, the IT environment for the TOE has changed to extend the range of hardware platforms on which the TOE is certified. None of these platforms has, however, required any change to the Trusted Solaris 8 code.

16. These changes are summarized in the sections below, based on the detailed analysis provided in the IAR [f]. For the most part, individual changes are uniquely identified by their *bugtraq* identifier. However, changes affecting only Base Solaris code are identified by their Solaris 8 patch identifiers. The reader should note that in many of these cases the patch identifiers relate specifically to SPARC machines, where equivalent x86 patches also exist; the latter are (for reasons of brevity) are not quoted. The analysis in all cases is supported by full regression testing. Where the analysis led to more specific changes these are noted in the 'Related Changes' column in the tables below.

Changes to TSP-Critical Code

17. A number of the bug fixes involve changes to TSP-critical code modules. Changes to this type of code have the greatest potential for undermining one or more SFRs, and therefore merited closest attention in order to confirm that they do not have a ***major*** impact. In each case the IAR [f] details the analysis performed by the Developer to confirm that the implementation of the SFRs is not adversely impacted. Changes are summarised in the table below.

Item	Description of change	Related changes
Unnecessary check for *proc_owner* privilege [4400301]	Corrected code to check for *proc_owner* privilege when a process accesses another subject only if the subject accessed has a different owner. This avoids having to grant the privilege to processes that do not otherwise need it.	Change to Filesystem LLD
Some kernel modules do not call correct TSOL security routines [4493976]	Replacement of **suser()** calls in kernel with appropriate Trusted Solaris checks.	Change to LLD Regression testing (all kernel tests) Minor change to a man page (bug 4770875)

Item	Description of change	Related changes
praudit and **auditreduce** command failures [4508276]	Redundant and incorrect access control checks removed. Affected code implements audit reduction capability.	Change to Audit LLD Regression testing of potentially impacted SF (Audit.19)
Failure to record full file path name in audit trail in some cases [4530450]	Corrected coding error. Affected code implements audit display capability.	Regression testing of potentially impacted SFs (Audit.6, Audit.19) Minor updates to test documentation
SunRay installation problem [4614171]	Though SunRay is outside the evaluated configuration, affected code implements lockscreen and trusted path SFRs.	Regression testing of potentially impacted SFs (IA.6-9, Tpath.7)
TCP connection failure [4635765]	Corrected by using a TSOL routine, passing the appropriate sensitivity label. Affected code implements MAC networking policy.	Change to Trusted Networking LLD Regression testing of impacted SF (MAC.26).
Panic caused in TCP by invalid destination address [4636041]	Corrected coding error. Affected code implements MAC networking policy.	Regression testing of potentially impacted SF (MAC.26).
Error in display of listed passwords for selection by user on first login [4640083]	Corrected coding error. Affected code implements login, password change, trusted path, subject labelling, and associated auditing SFRs.	Regression testing of potentially impacted SFs (IA.1-2, IA.8, IA.11-13, Tpath.2-5, Tpath.7, MAC.13, Audit.1, Audit.4).
System panic in kernel [4680438]	Corrected error in handling null VFS pointers. Affects call to code which implements DAC and MAC checks on file lookup.	Regression testing of MAC and DAC SFs
Vulnerability in **sessionetc** and **sessionexit** executing with incorrect security attributes. [4690160]	Removed vulnerability. Affected code implements trusted path and lockscreen SFRs.	Regression testing of potentially impacted SFs (Tpath.7, IA.6-7, IA.8-9).
TCP/IP vulnerability allowing attackers to eavesdrop a network by guessing Initial Sequence Numbers [4715170]	Removed vulnerability. Affected code implements MAC networking policy.	Regression testing of potentially impacted SF (MAC.26).
Buffer overflow in **login** [4727764]	Inserted check to prevent buffer overflow. Affected code implements login, password change, trusted path, subject labelling, and associated auditing SFRs.	Regression testing of potentially impacted SFs (IA.1-2, IA.4-5, IA.12-13, MAC.13, Tpath.2-5, Tpath.7, Audit.1).
Buffer overflow and other errors in **telnet** daemon [4734086] [4734108]	Appropriate checks inserted (though vulnerabilities not considered exploitable under Trusted Solaris). Affected code implements password encryption SFR.	Regression testing of potentially impacted SF (IA.8).
sendmail failure at start-up [4770747]	Fixed coding oversight. Affected code implements MAC and audit policy in respect of email.	Regression testing of potentially impacted SFs (MAC.1, MAC.2, MAC.3, MAC.4, Audit.3)
Xserver crash when using Netscape [4774192]	Fixed coding oversight. Affected code implements DAC and MAC checks, controls over changing labels, trusted path, and associated audit SFRs.	Regression testing of potentially impacted SFs (DAC.8, MAC.1-4, 6-7, 13-16, 18, Tpath.7, Audit.2-3, 6.)

Item	Description of change	Related changes
Denial of service exploit using /dev/tcp [4777250]	Fix ported from Solaris to TSOL. Affected code implements MAC networking policy.	Regression testing of potentially impacted SF (MAC.26)
Vulnerability allowing unprivileged processes to send raw IP packets out of the machine [4777620]	Fix ported from Solaris to TSOL. Affected code implements MAC networking policy.	Regression testing of potentially impacted SFs (MAC.17, MAC.25)
sendmail vulnerability allowing users to create files in root directory [4777623]	Fix ported from Solaris to TSOL. Affected code implements MAC and audit policy in respect of email.	Regression testing of potentially impacted SFs (MAC.1-4, Audit.3).
Potential IP spoofing vulnerability [4777815]	Disable IPv6 home address option by default. Affected code implements MAC and privilege networking policy SFRs.	Regression testing of potentially impacted SFs (MAC.17, MAC.25, MAC.9, OR.3, Priv.5)
Vulnerability in **netstat** command reporting port bindings for all labels [4778642]	Inserted check for *net_mac_read* privilege to view all port bindings at all labels. Affected code implements MAC networking policy.	Change to man page (bug 4793571) Change to Trusted Networking LLD Regression testing of potentially impacted SF (MAC.26).
Screen-stripe display of informational messages [4787041] [4790154]	Security irrelevant messages now displayed on screen stripe. Affected code implements login, trusted path, MAC policy on windows and subject labelling, and associated audit SFRs	Regression testing of potentially impacted SFs (MAC.7-8, MAC.13, MAC.21, Tpath.1-4, Tpath.6-7, Admin.5, Audit.1, Audit.4, IA.1-2, IA.11-13)
Inappropriate kernel uid 0 checks [4787676]	Replaced checks with TSOL privilege checks where appropriate	Update to man page (bug 4793575) Change to Filesystem and Devices LLD Regression testing of potentially impacted SFs.
Bug in copying directories by drag and drop [4804534]	Correct minor coding error. Affected code implements database access authorisation checks and audit (modification of security attributes and use of privilege) SFRs.	Regression testing of potentially impacted SFs (Admin.8, Audit.6-7)
License agreement text string [4805094]	Corrected. Affected code implements login, trusted path, MAC policy on subject labelling, and associated audit SFRs.	Regression testing of potentially impacted SFs (MAC.13, MAC.21, Tpath.1-4, Tpath.6-7, Audit.1, Audit.4, IA.1-2, IA.8, IA.11-13)
Various SunRay login and lockscreen problems [4805169] [4805172] [4811332] [4816925] [4868804]	Although SunRay is not part of the evaluated configuration, the affected code implements login, trusted path, MAC policy on subject labelling, and associated audit SFRs.	Regression testing of potentially impacted SFs (MAC.13, MAC.21, Tpath.2-5, Tpath.7, Audit.1, Audit.4, IA.1-2, IA.11-13)
Possible denial of service caused by TPI listener [4808989]	Correct TPI listener code to insert appropriate check. Affected code implements MAC networking policy.	Regression testing of potentially impacted SF (MAC.26)

Item	Description of change	Related changes
System panic caused by Multicast Listener Discovery messages. [4809041]	Move procedure call to appropriate place. Affected code implements MAC and Privilege networking policy checks.	Regression testing of potentially impacted SFs (MAC.17, MAC.25, MAC.9, OR.3, Priv.5)
Buffer overflow caused in **dtsession** [4809783]	Replaced inappropriate procedure call. Affects code that implements lockscreen and trusted path SFRs.	Regression testing of potentially impacted SFs (IA.6-9, Tpath.7).
Audit daemon failing to warn when threshold reached in some scenarios [4811567]	Audit daemon modified to check if audit full threshold has been crossed on startup, and to recheck if new threshold values are entered. Affected code implements auditing SFRs.	Change to Audit LLD Regression testing of potentially impacted SFs (Audit.1-14 and Audit.20-21).
Potential **sendmail** buffer overflow [4811604]	Corrected header parsing error. Affected code implements MAC and audit policy in respect of email.	Regression testing of potentially impacted SFs (MAC.1-4, Audit.3)
System panics caused in TCP stream module [4815350] [4836043] [4841926]	Corrected TCP data structures, added missing checks. Affected code implements MAC networking policy checks.	Regression testing of potentially impacted SF (MAC.26).
Memory leak problem in TCP and IP code [4819948]	Code corrected to free unneeded data structures. Affected code implements MAC and Privilege networking policy checks.	Regression testing of potentially impacted SFs (MAC.17, MAC.25, MAC.9, OR.3 and Priv.5)
Failure to check for audit trail saturation on start-up [4821612]	Inserted missing check in code. Affected code implements auditing SFRs.	Change to Audit LLD Regression testing of potentially impacted SFs (Audit.1-14, Audit.20-21, Audit.23)
Trusted screen-stripe display [4827810]	Change to display “Standard Edition” or “Certified Edition” in trusted stripe. Affected code implements lockscreen, trusted path, and MAC windowing policy SFRs.	Regression testing of potentially impacted SFs (MAC.7-8, MAC.21, IA.6-7, Tpath.1 and Tpath.6).
Buffer overflow in **sendmail** [4840218]	Added appropriate bounds checking. Affected code implements MAC and audit policy in respect of email.	Regression testing of potentially impacted SFs (MAC.1-4, Audit.3)
More restrictive policy for **ping** requested by some customers [4639031]	Code now permits use of **ping** only if the user label equals that of the remote system. Affected code implements MAC and Privilege networking policy checks.	Change to Trusted Networking LLD Regression testing of potentially impacted SFs (MAC.17, MAC.25, MAC.9, OR.3 and Priv.5).
X-server fails to start using certain extensions [4867023]	Corrected coding oversight. Affected code implements trusted path, DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18, Tpath.7, Audit.2-3 and Audit.6)

Item	Description of change	Related changes
Error in underlying algorithm causing failure to correctly parse some labels [4873497]	Algorithm used by label encoding parsing code corrected to handle all cases.	Regression testing of MAC SFs.
Auditing of new **update_drv (1M)** command [4880483]	Add new *AUE_update_drv* audit event so that the system call is audited. Affected code implements auditing SFRs.	Man page added for new command (bug 4899963 below) Change to Audit and Devices LLD Test documentation updated to test audit of new command, and regression testing of impacted SF (Audit.2). Transition Guide/Release Notes updated to describe new audit event
Review uid 0 checks in code ported from Solaris PSR3 [4880499]	Removed inappropriate uid 0 check (rendered unnecessary by TSOL privilege checks).	Regression testing of privilege SFs
Error in screen-stripe display showing system as “Not Licensed” [4881317]	Moved license file to prevent inadvertent deletion. Affected code implements lockscreen, trusted path and MAC policy on windowing SFRs.	Regression testing of potentially impacted SFs (IA.6-7, MAC.7-8, MAC.21, Tpath.1, Tpath.6)
Vulnerability in **tar** – files could be restored at wrong label [4885645]	Corrected coding error causing vulnerability. Affected code implements MAC policy on import/export and auditing of file restoration.	Regression testing of potentially impacted SFs (MAC.2, Audit.3).
Failure to handle blank lines in **audit_event(4)** file [4887617]	Check added to disregard white space. Affected file subject to audit data protection and administration SFRs.	Regression testing of potentially impacted SFs (Audit.14-16, Audit.18)
Automated test suite test failure owing to inappropriate privilege check [4893580]	Removed unnecessary check for *win_devices* privilege in **Xsun(1)**. Affected code implements trusted path, DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18, Tpath.7, Audit.2-3 and Audit.6)
Customer-requested tightening of network security policy [4894365]	New function added to ensure applications using TCP or UDP will not send packets over the wire unless the user label is equal to that of the remote non-Trusted Solaris system, if required. (More restrictive than the Security Target requires.) Affected code implements MAC networking policy checks.	Change to Trusted Networking LLD Regression testing of potentially impacted SF (MAC.26).
Problem using Sun Type 6 USB keyboards [4903657]	Adjustment to accommodate mapping of the keys. Affected code implements trusted path, DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18, Tpath.7, Audit.2-3 and Audit.6)

Item	Description of change	Related changes
Lockscreen fails to work when submenu in a menus bar is displayed (e.g. through right-click action) [4903672]	Corrected coding oversight. Affected code implements lockscreen, trusted path, and the DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (IA.6-9, DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18, Tpath.7, Audit.2-3 and Audit.6.)
Error in license status display in screen-stripe on freshly installed system [4909783]	Corrected coding oversight. Affected code implements DAC and MAC policy on windows objects, lockscreen, and trusted path SFRs.	Regression testing of potentially impacted SFs (MAC.7-8, MAC.21, IA.6-7, Tpath.1, Tpath.6 and Admin.5).
Infinite loop bug in **allocate** code [4910923]	Increased buffer size to accommodate a long entry for devices. Affected code implements MAC and audit policy on devices.	Regression testing of potentially impacted SFs (MAC.19-20 and Audit.10)
Problems accessing NFS file systems [4915227]	Corrected bug in stream head creation to ensure that correct security attributes are used.	Change to Filesystem LLD Regression testing (network tests)
Lockscreen vulnerability in SunRay configuration [4920664]	Although SunRay is not part of evaluated configuration, the change affects code that implements lockscreen and trusted path SFRs.	Regression testing of potentially impacted SFs (IA.6-9, Tpath.7)
Vulnerability in **tar** that could expose previously stored data [4925103]	Fix to ensure previous data correctly overwritten. Affected code implements MAC policy on import/export and auditing of file restoration.	Change to Devices LLD Regression testing of potentially impacted SFs (MAC.2, Audit.3).
sendmail buffer underflow vulnerability [4927826]	Added missing checks to code. Affected code implements MAC and audit policy in respect of email.	Regression testing of potentially impacted SFs (MAC.1-4, Audit.3)
Vulnerability in **df** command, permitting exposure of filesystem information [4931908]	Added a new routine, *secpolicy_fs_access*, to perform appropriate MAC and DAC checks.	Change to Filesystem LLD Test documentation updated
Vulnerability from insecure creation of temporary files by applications using Direct Graphics Access (DGA) on Sparc machines [4933122]	Back-port of Solaris security bug. Affected code implements trusted path, DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18, Tpath.7, Audit.2-3 and Audit.6)
dtsession dies in SunRay configuration [4939675]	Although SunRay is not part of the evaluated configuration, the bug fix changes code that implements lockscreen, and trusted path SFRs.	Regression testing of potentially impacted SFs (IA.6-9, Tpath.7).
Modification of user account overwrites time of last password change field [4766108]	Corrected coding oversight in SMC User Manager code. Affected code implements user account administration SFRs.	Regression testing of potentially impacted SFs (IA.3, 6, 7, 9, Admin.7 and Audit.1)
sendmail buffer overflow [4954379]	Fixed buffer overflow. Affected code implements MAC and audit policy in respect of email.	Regression testing of potentially impacted SFs (MAC.1, MAC.2, MAC.3, MAC.4, Audit.3)

Comment: Start of 2/04 changes

Item	Description of change	Related changes
Customer-requested enhancement enabling customisation of Window Workspace menu. [4956889]	Enhancement modifies code that implements MAC and DAC policy on windows objects, lockscreen and trusted path SFRs.	Regression testing of potentially impacted SFs (MAC.7-8. MAC.21, Tpath.1, 6, IA.6-7 and Admin.5) TS 8 02/04 Release Notes updated to explain the new feature
Ensure privilege checks made only when needed [4965212]	Changed order of checks. (This change improves privilege-debugging, helping to ensure system integrators do not grant un-needed privileges to site-specific programs when configuring the system.)	Regression testing of Privilege SFs
Adding user with non-existent home directory renders system unusable [5016883]	Corrected error handling code. Affected code implements authorisation checks on role assignment and file security attribute changes.	Regression testing of potentially impacted SFs (Admin.4, Admin.6)
Lockscreen failure in SunRay configuration [5033132]	Although SunRay is not part of the evaluated configuration, the bug fix modifies code that implements lockscreen, and trusted path SFRs.	Regression testing of potentially impacted SFs (IA.6-9, Tpath.7).
Vulnerability in TSOL Windowing code [5040043]	Added appropriate checks for invalid UIDs. Affected code implements trusted path, DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18; Tpath.7; Audit.2-3, Audit.6.)
Deadlock in network stack observed in some scenarios [5044793]	Correction of handling of locks. Affected code implements MAC and Privilege network policy checks.	Regression testing of potentially impacted SFs (MAC.9, MAC.17, MAC.25; OR.3, Priv.5)
Duplicate audit mask values result in certain events being audited when not requested [6212255]	Corrected **audit_class** file to remove duplicate masks. This file is subject to audit data protection SFRs.	Regression testing of potentially impacted SFs (Audit.14, Audit.16).
Vulnerability in remote system log-off resulting in exposure of previous session content [6236207]	Corrected code implementing exiting signal on log-off. Affected code implements login, trusted path, MAC policy on windows and subject creation, and associated audit SFRs.	Regression testing of potentially impacted SFs (IA.1-2, IA.8, IA.11-13, Tpath.2-5, Tpath.7; Audit.1, Audit.4; MAC.13, MAC.21)
Potential vulnerability in ftp daemon failing to switch off privileges when not needed [6264842]	Corrected coding error **in.ftpd**. Affected code implements login, and associated audit SFRs.	Regression testing of potentially impacted SFs (Audit.1, 4; IA.1-2, IA.4-5, IA.11)
Various bugs in **Xsun(1)**, mostly security irrelevant but including a small number of vulnerabilities (including buffer overflows) [Patch 108652-74]	Vulnerabilities and other coding problems fixed. Affected code implements trusted path, DAC, MAC and audit policy on accesses to windows objects.	Regression testing of potentially impacted SFs (DAC.8-9, MAC.1-4, MAC.6-7, MAC.13-16, MAC.18, Tpath.7, Audit.2-3 and Audit.6)

Item	Description of change	Related changes
Various bugs in **dtlogin(1)** [Patch 108919-20] Various bugs (non-security related) in **dtwm(1)** [Patch 108921-17] [Patch 108923-01]	Corrected problems in code. Affected code implements login, password change, trusted path, subject labelling, and associated auditing SFRs. Corrected problems in code. Affected code implements trusted windowing, lockscreen and trusted path SFRs.	Regression testing of potentially impacted SFs (Audit.1, Audit.4, IA.1-2, IA.6-9, IA.11, IA.12-13, MAC.13, MAC.21, Tpath.2-5, Tpath.7) Regression testing of potentially impacted SFs (MAC.7-8, MAC.21, Tpath.1, Tpath.6, IA.6-7, Admin.5)
Vulnerability in **in.rshd(1M)** allowing connections to unprivileged ports [Patch 108985-03]	Vulnerability and other coding errors fixed. Affected code implements remote login SFRs.	Regression testing of potentially impacted SFs (IA.1, IA.8)
Various LDAP related bug fixes, including a number of buffer overflows and race conditions [Patch 108993-31] Error in implementation of security irrelevant options to **useradd**, **userdel** and **usermod** commands [Patch 109035-02]	Corrected problems in code. Affected code implements login, password change, trusted path, subject labelling, and associated auditing SFRs. (Note however that LDAP is not within the evaluated configuration.) Corrects coding errors. Affected code implements user account management SFRs.	Regression testing of potentially impacted SFs (Audit.1, Audit.4, IA.1-2, IA.8, IA.11, IA.12-13, MAC.13, MAC.21, Tpath.2-5, Tpath.7) Regression testing of potentially impacted SF (IA.9)
Various problems relating to login, logout and session locking, including a small number of vulnerabilities, in **dtsession(1)**. [Patch 109354-19]	Corrected problems in code. Affected code implements lockscreen and trusted path SFRs.	Regression testing of potentially impacted SFs (IA.6-9, Tpath.7)
Various bugs in **sendmail(1M)**, including a buffer overflow. [Patch 110615-10] Fixes several bugs, including buffer overflow and denial of service vulnerabilities in **in.telnetd(1M)**. [Patch 110668-04]	Corrected problems in code. Affected code implements MAC and audit policy in respect of email. Corrected problems in code. Affected code implements remote login SFRs.	Regression testing of potentially impacted SFs (MAC.1-4, Audit.3) Regression testing of potentially impacted SF (IA.8)
Security irrelevant bugs in **tar(1)** command. [Patch 110951-04]	Corrects coding errors. Affected code implements MAC policy on import/export and auditing of file restoration.	Regression testing of potentially impacted SFs (MAC.2, OR.1, Audit.3).
Vulnerabilities in **in.ftpd(1M)**. [Patch 111606-04] [4392163] [5108531]	Fixes vulnerabilities. Affected code implements remote login and associated audit SFRs.	Regression testing of potentially impacted SFs (Audit.1, 4; IA.1-2, IA.4-5, IA.11)
Security irrelevant bugs in **rem_drv** command. [Patch 111804-03]	Corrects coding errors. Affected code implements Auditing SFRs.	Regression testing of potentially impacted SFs (Audit.15-16)

Item	Description of change	Related changes
Role deletion bug in **passmgmt** command [Patch 112993-01]	Corrects coding error. Affected code implements user account management SFRs.	Regression testing of potentially impacted SFs (IA.9)

Table 1: Summary of Changes to TSP-Critical Code

18. The Certification Body has examined the IAR [f] and accepts that evidence provided demonstrates that each of the above changes is ***minor***. Where the change involved modifications to the low-level design, the Certification Body supplemented examination of the IAR with inspection of the design updates and of the modified code itself to confirm that the impact was indeed ***minor***.

Changes to TSF to remove vulnerabilities

19. The following table provides a summary of changes to TSP-supporting code (that is, code that is part of the TSF but which does not directly implement any SFR) to remove potential or actual vulnerabilities (typically buffer overflows or system panics that potentially lead to denial of service). See also Table 8 below, which identifies various patches to Base Solaris that have been incorporated in Trusted Solaris 8 2/04, and which affect TSP-supporting code. These include fixes to a number of vulnerabilities reported in Solaris 8.

Item	Description of change	Related changes
Panic in networking code [4529093]	Inserted appropriate checks	[None]
Buffer overflow in **dtspcd** library function [4531945]	Inserted appropriate checks	[None]
Memory leak caused by **automountd** [4614049]	Released data structure when not needed.	[None]
man command leaves temporary files [4623549]	Corrected code to remove temporary files.	[None]
Mail buffer overflow [4668266]	Inserted appropriate checks	[None]
Potential vulnerability that could cause **sendmail** to execute arbitrary commands. [4668341]	Corrected routine call to remove the vulnerability	[None]
IPv6 port binding vulnerability invalidating MAC policy [4671056]	Corrected code to ensure client and server communications are confined to the same sensitivity label.	[None]
System panic in kernel [4673336]	Corrected faulty algorithm	[None]
System panic in kernel caused by **mount** system call [4673342]	Corrected data structures and inserted appropriate checks	[None]

Item	Description of change	Related changes
Unsafe (predictable) creation of temporary files by **vi**. [4690096]	Changed routine call to create files with random names	[None]
Vulnerability in use of environment variables potentially allowing untrusted code to be run under a trusted UID [4701212]	Corrected code to ignore unsafe environment variables	[None]
Buffer overflow in **xlock** command [4704255]	Corrected checks in code	[None]
Buffer overflow during login [4727764]	Inserted appropriate checks (in TSF-supporting code).	[None]
Buffer overflow using RPC services [4730100]	Inserted appropriate checks.	[None]
System panic in kernel [4809718]	Corrected code to prevent unexpected use of floating point operations	[None]
Deadlock and panic in kernel [4771519]	Reversed lock ordering	[None]
Various buffer overflows, race conditions [4777214] [4777221] [4777224] [4777237] [4777241] [4777244] [4777248] [4777627] [4777709] [4777724] [4777825]	Fixes ported from Solaris to TSOL.	Update to Developer Vulnerability Analysis
Vulnerability in **priocntl** system call enabling attacker to gain root access [4777632]	Fix ported from Solaris to TSOL	[None]
Vulnerability in use of **ed** command – insecure creation of temporary files [4777716]	Fix ported from Solaris to TSOL.	[None]
Vulnerability in use of sysinfo function allowing unauthorised access to kernel information [4777862]	Fix ported from Solaris to TSOL	[None]
Insecure creation of temporary files by **fbconsole** leads to race condition and potential symlink attack [4777864]	Fix ported from Solaris to TSOL	[None]

Item	Description of change	Related changes
System panic in kernel [4788513]	Corrected faulty calculation leading to illegal values	[None]
System panic in kernel [4808657]	Corrected code (missing while loop)	[None]
Multiple remote vulnerabilities in BIND CERT Advisory [4808854]	Corrected code to remove potential buffer overflows	[None]
ftp debug output includes passwords in clear text [4808889]	Corrected code to display XXXX instead of password	Update to Developer Vulnerability Analysis
Buffer overflow in **uucp** command [4808899]	Corrected handling of buffer	[None]
Race condition and potential vulnerability allowing unexpected file removal using **at** command [4808901]	Inserted appropriate checks	[None]
Buffer overflow in use of RPC services [4809705]	Inserted appropriate checks	[None]
Buffer overflow in Trusted Windowing [4809772]	Changed procedure call	[None]
KCMS (Kodak Colour Management System) known to be vulnerable [4815087]	Disabled service.	[None]
Segmentation violation potentially exploitable to gain root access [4874204]	Inserted appropriate checks	[None]
Memory leakage in **rpc.nisd**. [4905191] Remove buffer overflow in LDAP libraries [4905402]	Correct coding error Replaced unsafe routine call. Note that LDAP is not part of the evaluated configuration.	[None] [None]
Denial of service through user-initiated kernel panic, or corruption of kernel address space [4905554]	Correct code so that system uses its own kernel data structure.	[None]
Buffer overflow in **rpc.nisd**. [4906223]	Replaced unsafe routine call.	[None]
Buffer overflow in audit support code [4906298]	Inserted appropriate argument checks	[None]
System panic when **edition** module is unloaded. [4909278]	Corrected coding error	[None]
File descriptor leak by **nscd** [4913010]	Removed part of fix to bug 4905191 that introduced this problem, enabling file descriptors to be reused when no longer needed.	Bug 4905191 (above)

Item	Description of change	Related changes
Potential user-initiated kernel panic and memory corruption. [4913087]	Ported fix from Solaris to correct code.	[None]
Vulnerability in **format** command could be exploited to gain root access [4914644]	Correct code to prevent user escaping from shell	[None]
Vulnerability in **priocntl** allowing arbitrary code to be injected into the kernel. [4918003]	Inserted appropriate checks in code	[None]
sadmind daemon is potentially vulnerable. [4922947]	Disabled daemon (which is no longer needed)	[None]
proc tool command error messages allow unprivileged processes to infer information about the label of other processes. [4932041]	Corrected code to mask error messages that could contravene the MAC policy	[None]
Buffer overflow in Window Manager Help function. [4933212]	Replaced unsafe procedure call	[None]
Port 898 vulnerability permits attacker to infer whether a file exists on systems acting as SMC web server. [5074119]	Back-port fix from Solaris	[None]
TSOL8 HW 7/03 upgrade problem, replacing authentication modules with unevaluated modules. [5075722] [6248413]	Correct installation code to prevent replacement of **pam** modules	[None]
Buffer overflow in **dtmail** [6182112]	Corrected unsafe function call	[None]
System panic when an empty undersized packet is sent to a labelled system. [6224841]	Corrected error in networking code.	[None]
Bogus IP address included in **tnrhdb** file during installation process [6238576]	Corrected code to ensure bogus IP address is not included	[None]
System hangs at some customer sites due to audit queue buffer filling [6250977]	Increased size of audit queue buffer.	[None]

Table 2: Summary of TSP-Supporting Code Vulnerability Fixes

Changes to TSF that affect security functionality

20. The following table provides a summary of changes to TSP-supporting code that affect security functionality in some way. Generally these are requests by customers to improve usability, or to enforce additional security policy restrictions that are beyond those required by the Security Target [c].

Item	Description of change	Related changes
Window manager crash when selecting invalid label during downgrade process. [4927901]	Inserted code to properly handle invalid label error condition	[None]
Label Selection Tool prevents un-setting of previously selected compartments [4927903]	Corrected typographical error in Label daemon code.	[None]
Inadequate label validity checking in Label daemon [4932668]	Inserted check for case where specified minimum clearance is not a valid label	[None]
Customer-requested tightening of security policy preventing any traffic over the wire relating to file requests that will be denied [4926203]	Changed automount daemon to look up label of remote file server, and not mount the remote file system if subsequent file requests will be denied by the MAC policy (remote file system dominates process label and process does not hold the requisite privileges). Note: these checks are not actually required by the Security Target.	Change to Filesystem LLD
Customer-requested tightening of security policy preventing any traffic over the wire relating to file requests that will be denied [4934078] [5045660]	Changed code to enable checks to be performed to determine whether access will be permitted, before any traffic goes over the wire. Note: these checks are not actually required by the Security Target.	Change to Filesystem LLD
Replicated mount problems, despite previous two fixes [5016234] [5028607]	Include pre-emptive check on label of remote file system in code path overlooked during previous two fixes. Note: these checks are not actually required by the Security Target.	Bugs 4926203, 4934078, 5045660
Tightening of ping policy prevents TSF locating and auto-mounting remote file servers in certain configurations [5018531]	Privilege added to automount daemon if option of tightening policy on use of ping is adopted (as per bug 4639031)	Bug 4639031 Change to Filesystem LLD
Inadequate label input checking/error reporting by label daemon [6248431]	Corrected code to check whether classification value is greater than maximum allowed value. Note that this fix improves usability: there was no vulnerability.	[None]

Table 3: Summary of Security Relevant Changes to TSP-Supporting Code

Changes to man pages

21. The following table provides a summary of changes to man pages for specific commands, where there was an identified need to ensure the information presented is current and accurate. In some cases this was to correct or update security relevant information, for example in the description of privileges needed to execute commands.

Item	Description of change	Related changes
wall(1M) man page [4364334]	Updated to correctly reflect use of privileges	[None]
mnttab(4) man page [4770875]	Reverted to Solaris man page following bug fix	Bug 4493976
processor_bind(2) man page [4774080]	Updated to provide missing TSOL relevant information	[None]

man pages for **fssnap(1M)**
fssnap_ufs(1M)
wrsmconf(1M)
wrsmstat(1M)
pmconfig(1M)
[4782247]
	Updated to describe privileges needed for successful operation	[None]

praudit man page [4782730]	Corrected inaccuracies in description	[None]
netstat(1m) man page [4793571]	Updated to state that *net_mac_read* privilege is required to see all port bindings at all sensitivity labels	Bug 4778642
llc2(7D) man page [4793575]	Updated to reflect kernel uid 0 check	Bug 4787676
prtconf(1M) man page [4797012]	Updated to reflect modified behaviour	[None]
mount(2) man page [4797526]	Corrected description of command (security irrelevant)	[None]
audit_user(4) man page [4799928]	Updated to reflect restrictive permissions on **audit_user** NIS+ table	[None]
pkgadd(1M) man page [4801304]	Updated to state privileges required under TSOL	[None]
setfsattr(1M) man page [4817080]	Updated to clarify behaviour with respect to handling of file security attributes	[None]
update_drv(1M) man page [4899963]	Updated man pages to include new command	Transition Guide/Release Notes describes new audit event. Bug 4880483
device_deallocate(4) man page [4924428]	Removed man page (obsolete command).	Removed references to command from AnswerBook
kadb(1m) man page [4924707]	Updated to include power management information.	[None]
mount_ufs(1m) and **mount_nfs(1m)** man pages [4926878]	Updated to most current and accurate state	[None]

Comment: Start of HW 07/03 changes

Item	Description of change	Related changes
audit_event(4) and **audit_class(4)** man pages [4938230]	Updated to most current and accurate state.	[None]
Corrections to various Base Solaris man pages [Patch 108808-44] [Patch 108897-01]	These corrections have no impact on any security functionality, with one exception: an enhancement to the documentation of one of the options to the **useradd** command.	[None]

Table 4: Summary of Changes to man pages

Changes to command privileges or user profiles

22. The following table provides a summary of changes to the privileges assigned to commands, or to the privileges or commands associated with particular user profiles. In all cases the motivation for these changes is to enable the relevant functions to work under Trusted Solaris.

Item	Description of change	Related changes
All executable files [4440204]	Assignment of privileges to executables during operating system installation achieved by more reliable method to ensure correct installation of any additional software packages.	[None]
rpc.nisd [4640822]	Privilege added to prevent erroneous timed out message.	[None]
tsolinfo file [4768573]	Attributes for roles no longer provided by default are removed	[None]
Boot profile [4783646] [4795360] [4803233]	Added **wrsmconf** and **kdmconfig** commands to profile Added *priv_sys_config* and *sys_devices* privileges to profile	[None]
nisserver command [4797661]	Added *sys_config* privilege to command	[None]
Boot profile [4784532]	Added *file_chown* privilege to **syseventd** to correct problem that limited the number of logins to 32	[None]
Software installation profile [4799303]	Corrected CD image path	[None]
inetd profile [4806666]	Updated privileges to ensure SunRay programs can be launched by SunRay web server (not part of evaluated configuration).	[None]
ypinit command [4824618]	Added *net_privaddr* and *sys_net_config* privileges to command.	[None]
cvcd command **sckmd** command [4825132]	Added *net_mac_read* and *net_reply_equal privileges* to **cvcd**; and *sys_net_config privilege* to **sckmd**.	[None]

Item	Description of change	Related changes
add_install_client, **rm_install_client** installation scripts [4830583]	Added *proc_owner* privilege to scripts.	[None]
Boot and inetd profiles [4835696]	Changed profiles for SunFire 15K systems.	[None]
Maintenance and Repair profiles [4837675]	Added **cfgadm** command to profiles for Dynamic Reconfiguration (not within the scope of evaluation).	[None]
SunRay Management Profile [4826446] [4877087]	Added missing privleges to, and corrected typo in, profile. SunRay is not within the evaluated configuration	[None]
inetd profile [4878800] File System Management profile [4937542]	Updated to enable **in.rlogind** and **in.telnetd** to generate proper wtmpx database entries (holding history of user access and administrative information). Added missing privileges for **format** and **eject**.	[None] [None]
Software Installation profile [4894549] Software Installation and Sun Ray Initialisation profiles [6237910] [5096091] [6178344]	Add correct pathname to install CD Corrections to profiles (the latter is not relevant to the evaluated configuration).	[None] [None]

Table 5: Summary of Changes to Command Privileges or User Role Profiles

Changes to fix Installation or Build problems

23. The following table provides a summary of changes to code or scripts involved in installing or upgrading Trusted Solaris or optional packages.

Items	Description of change	Related changes
Development tools [4451773]	Fixed problem in security irrelevant tool used in support of testing fixes	[None]
Patch installation [4529386]	Prevented misleading error messages when installing non-TSOL patch	[None]
Package installation [4765225] [4771397] [4791524] [4798752] [4801298] [4925190]	▪ Provided missing DHCP help files (not in the scope of evaluation) ▪ Fixed coding oversight ▪ Fixed failure in /dev/random installation ▪ Corrected package-compare script ▪ Fixed checks and memory leak ▪ Included missing shared library	Bug 4750495 (/dev/random feature)

Items	Description of change	Related changes
CD installation [4775067]	Modified installation start-up script to ask for second CD	[None]
Merge program [4763243]	Corrected use of strings to ensure messages displayed on calendar icon	[None]
Build process [4787218]	Added missing header files to enable successful compilation of TSOL sources	[None]
Build scripts [4791044]	Corrected error in nightly build process in TSOL development environment	[None]
CDE installation tools [4799458]	Corrected CD image pathname	[None]
Post-install script [4801528]	Updated device list to ensure all devices protected by admin-high label	[None]
Post-install and Post-remove scripts [4810630]	Added missing scripts for certain packages.	[None]
analyze_patch script [4817768] Patch installation [4837454]	Corrected error in OS release directory name. Corrected error in calculation of free-space	[None] [None]
Upgrade installation code [4907388]	Corrected error causing failed upgrades from Trusted Solaris 7.	[None]
Makefile [4907817]	Fixed large-file support for **chgrp**, **chmod** and **chown** commands.	[None]
SunScreen installation [4920718]	Corrected in **device_policy** file causing panic during installation.	[None]
Solaris Linker [5077438]	Fixed bug that causes SMC Server crash	[None]

Table 6: Summary of Changes to Fix Installation or Build Problems

Security Irrelevant Changes

24. The following table provides a summary of changes to TSP-supporting or security irrelevant code, generally to remove security irrelevant bugs. See also Table 9 below, which covers changes to security irrelevant code in Base Solaris.

Item	Description of change	Related changes
Errors handling files and symbolic links [4087003] [4868574] [4877950]	Corrected coding errors in **updatehome(1M)** and **mldrealpath(3tsol)** commands	[None]
lint errors in libraries [4430859]	Corrected to satisfy lint restrictions	[None]
Device allocation manager GUI failure [4533649]	Corrected coding error	[None]

Item	Description of change	Related changes
TSOL as CIPSO router problem [4599464]	Fixed security-irrelevant coding error handling CIPSO (Common IP Security Option) options	[None]
File locking problem [4630155]	Corrected code to ensure **statd** has the requisite privileges (as per man page)	[None]
Improved random number generation support [4750495]	Added new feature (**/dev/random**) to improve quality of random numbers generated for applications (not used by any SFs)	[None]
Message queue display error [4753421]	Used correct TSOL data structures for display	Minor updates to test documentation
SMC server fails to start [4762929]	Fixed coding error	[None]
TSOL system call display error [4770655]	Fixed error in **truss** command	[None]
Core dump using **ptree** [4774605]	Fixed coding error **ptree** command	[None]
Various SunRay problems [4787665] [4830589] [4830611] [4868842] [5020313] [5026455] [5038488] [5066620]	Fixed various SunRay installation and login problems. SunRay is not within the evaluated configuration.	[None]
Errors in implementation of NFS interfaces [4814632] [4814645]	Corrected security irrelevant deficiencies in implementation of various options for documented NFS interfaces.	[None]
/etc/release file [4880168]	Corrected typographical error.	[None]
Support for new hardware (V1280) [4880491] [4912848]	▪ Ported missing code from Solaris 9. ▪ Increased buffer size for **deallocate** command.	[None]
Syslogd failing to log to remote hosts [4898790]	Corrected coding oversight to cater for case where file descriptor points to remote host, relying on network security policy code to make appropriate checks.	[None]
Automated test suite [4899579]	Improvement in **tar** test suite procedures.	[None]
CDE access control menu items fail [4904417]	Added missing path to **Xtsolusersession** shell script.	[None]
Incorrect usage message [4939666]	Corrected usage message displayed by **tsol_dev_policy** and **tsol_priv_enable** .	[None]
Remote print failures (side effect of network policy tightening) [5032544]	Modified implementation of **libprint** to allow it to comply with the tightened policy.	[None]

Item	Description of change	Related changes
Automountd coding error [5056435]	Corrected coding error.	[None]
Users unlocked by administrator not required to set password for min age days [5070621]	HW 7/03 fix removed by subsequent Solaris bug fix: no security impact.	[None]
Duplicate entry in **exec_attr** file [5074088]	Removal of duplicate Device Security line.	[None]
Various Apache vulnerabilities [6191815] [6215421]	Fixed vulnerabilities (Apache is not enabled in the evaluated configuration).	[None]
Error parsing **tcsh** command inputs [6237916]	Corrected coding error	[None]
Deallocation of CD-ROM fails in certain scenarios [6238532]	Corrected error in **disk_clean** script	[None]
Copyright string [6239033]	Updated copyright string in **/etc/release** and as displayed in boot-up message	[None]
Un-mount failures [6246386] [6246747]	Corrected vnode reference count error causing TOE to incorrectly think the file system was still in use.	[None]
False reporting of faulty RMC cards [6258998]	Fixed error in unloading of **su** driver that caused the problem.	[None]

Table 7: Summary of Fixes to Security Irrelevant Bugs

Base Solaris Changes affecting TSP-Supporting Code

25. The following table provides a summary of changes to TSP-supporting code in Base Solaris 8. Generally these changes are intended to remove security irrelevant bugs; however, as noted in the table below, a minority of changes are to remove detected vulnerabilities (typically buffer overflows and system panics).

26. Except where otherwise stated, all references in Tables 8 and 9 are to Solaris Patch IDs. For the most recent Base Solaris changes, bug IDs are quoted instead.

Item (Patch ID)	Description of change	Related changes
108529-29, 108956-08, 108693-06, 108974-33, 108981-12, 108983-08, 108984-08, 108989-02, 109189-05, 109374-06, 109458-03, 109460-10, 109793-23, 109815-19, 109893-04, 109896-21, 109898-05, 109922-04, 109924-04, 110075-01, 110320-03, 110374-08, 110375-05, 110461-03, 110820-10, 110823-04, 110824-04, 110826-09, 110836-05, 110837-05, 110842-11, 110848-02, 110867-01, 110900-09, 110901-01, 110953-04, 110955-04, 111304-01, 111321-03, 111335-20, 111588-04, 111741-02, 111790-17, 111831-01, 111881-03, 112077-08, 112119-04, 112158-04, 112170-02, 112229-04, 112254-01, 112609-02, 112798-01, 113685-05, 113687-01, 114162-01, 114583-01, 115576-01	Various kernel/driver update patches. The majority of bug fixes covered by this patch are security irrelevant; however a number of vulnerabilities are covered by these patches as well (including some buffer overflows, race conditions, and instances of memory corruption). All patches affect code in the kernel, which is TSP-supporting.	[None]
108576-45, 108604-34, 108605-35, 108606-33, 109154-20, 109582-02, 109862-03, 110127-04, 110750-01, 111852-01, 114357-19, 114554-12	Non-security related graphics patches affecting TSP-supporting code in the kernel	[None]
108723-01, 108727-25, 108820-02, 108823-01, 108835-04, 108964-06, 108970-01, 108972-04, 108975-08, 109091-06, 109454-02, 109576-01, 109764-04, 109783-02, 110283-06, 110387-05, 110898-08, 110903-05, 110910-02, 110943-01, 110945-08, 111023-03, 111197-02, 111439-02, 111548-01, 112325-01, 112425-01, 113648-03, 114671-01, 114984-01 Bugs: 4353832, 4509659, 4671383, 4723351, 4789213, 4803148, 4889619	Fixes to various file system bugs. The majority of these are not relevant to security. However, the patches include a small number of security-related bug fixes (e.g. race conditions, buffer overflows, vulnerabilities in the handling of temporary files, etc.).	[None]

Item (Patch ID)	Description of change	Related changes
108725-14, 108806-17, 108813-16, 108982-09, 109872-01, 109876-02, 109879-02, 109882-06, 109883-02, 109885-14, 109892-04, 109894-01, 109920-09, 109926-02, 109928-05, 110088-02, 110150-04, 110221-07, 110285-02, 110368-02, 110369-05, 110371-03, 110373-05, 110379-01, 110382-03, 110369-05, 110614-02, 110723-06, 110821-02, 110822-01, 110825-03, 110828-02, 110829-02, 110831-02, 110832-01, 110835-06, 110840-03, 110841-01, 110844-02, 110845-03, 110846-02, 110847-02, 110851-02, 110852-03, 110854-02, 110918-06, 111018-01, 111041-04, 111498-04, 111657-01, 111789-04, 111883-20, 111995-06, 112001-08, 112162-03, 112163-01, 112164-01, 112168-02, 112169-01, 112172-02, 112173-01, 112174-01, 112369-01, 112438-02, 112794-01, 112849-01, 112850-01, 113501-01, 113654-01, 113679-05, 113680-03, 113681-03, 113682-02, 113683-02, 114157-01, 115275-02	Driver patches (non-security related). These affect TSP-supporting code in the kernel.	[None]
108869-22, 108940-57, 108949-07, 109951-01, 110269-01, 110322-02, 110380-04, 110416-03, 110458-02, 110794-05, 110896-02, 111049-03, 111302-03, 111306-05, 111308-04, 111310-01, 111325-02, 111327-05, 111332-08, 111626-03, 111647-01, 111791-02, 111796-04, 112135-01, 112159-02, 112459-01, 112611-02, 112792-01, 112846-01, 113242-01, 113650-02, 113655-03 Bugs: 4471907, 4500613, 4617431, 4863307, 4879704, 4879822, 4933407, 4941011, 5086486, 5086488, 5092678, 5098146, 6182042	Fixes to various problems in TSPsupporting libraries (this includes a number of buffer overflows).	[None]
109077-02, 109202-05, 109326-13, 109328-03, 109900-02, 109902-03, 110378-06, 110511-05, 110670-01, 110839-04	Fixes to various networking-related problems, including some vulnerabilities (segmentation violations, deadlock).	[None]

Item (Patch ID)	Description of change	Related changes
109142-07, 109145-01, 109147-26, 109149-02, 109277-03, 108609-01, 109727-01, 109729-01, 109933-02, 110386-03, 110702-01, 110710-01, 110934-14, 111317-05, 111382-01, 111697-04, 112097-03, 112501-01, 112607-02, 113749-01, 114675-01, 114956-02, 115827-01	Fixes to various security irrelevant problems that affect TSPsupporting code.	[None]
108714-08	**CDE 1.4: libDtWidget** patch. Fixes a number of security irrelevant problems together with some permissions/ownership vulnerabilities.	[None]
108899-04	Fixes to **ftp** (including clear-text password vulnerability, bug 4808889 described in table 2 above)	Bug 4808889
108987-13	**patchadd**/**patchrm** patch, which includes a fix to a potential vulnerability (failure to clean up temporary files)	[None]
108999-01 Bugs 4873939, 4887906, 4977110	**pam** patch. This fixes a small number of security irrelevant bugs.	[None]
109007-13	**at**/**atrm**/**batch**/**cron** patch. Fixes a number of bugs, including some auditing problems relating to the use of these commands.	[None]
109134-28	**wbem** patch. This fixes a large number of problems, including a small number of vulnerabilities (mostly relating to allocation or misallocation of privileges). WBEM is not within the evaluated configuration.	[None]
109152-02	**dbmopen**/**dbminit** patch. Removes a buffer overflow.	[None]
109238-02	**ipcs** patch. Fixes a vulnerability (segmentation violation)	[None]
109320-06	**lp** patch. Fixes a number of bugs, including a small number of print-related vulnerabilities.	[None]
109324-05	**sh**/**jsh**/**rsh**/**pfsh** patch. Fixes a small number of vulnerabilities (segmentation violation, predictable temporary files)	[None]
109667-05	**xntpd**/**ntpdate** patch. Fixes various timer/clock related problems, including one buffer overflow.	[None]
110453-04	**admintool** patch. Fixes several buffer overflows.	[None]
110957-02, 111874-06, 113792-01	**mail/mailx/mailtool** patches. Fixes vulnerabilities.	[None]
111069-01	**bsmunconv** patch. Fixes a vulnerability.	[None]
111071-01	**cu** patch. Fixes a buffer overflow.	[None]
111232-01, 111234-01	**in.fingerd/finger** patches. Fixes two vulnerabilities.	[None]

Item (Patch ID)	Description of change	Related changes
111269-03	**SMC** patch. Fixes an error in a TSP-supporting part of SMC.	[None]
111400-02	**KCMS configure tool** patch. Fixes a vulnerability in the KCMS daemon.	[None]
111504-01	**tip** patch. Fixes a number of vulnerabilities.	[None]
111570-02	**uucp** patch. Fixes a buffer overflow.	[None]
111596-03	**yppasswd** patch. Fixes a buffer overflow.	[None]
111624-04	**inetd** patch. Fixes a number of bugs including one security related issue (generation of a duplicate audit record).	[None]
111826-01	**whodo** patch. Fixes a buffer overflow.	[None]
112039-01	**ckitem** patch. Fixes potential stack overflow.	[None]
112668-01	**gzip** patch. Fixes security issue.	[None]
112796-01	**in.talkd** patch. Fixes vulnerability.	[None]
112991-01	**prtvtoc** patch. Fixes segmentation fault.	[None]
112996-01	**sysconf** patch. Fixes permissions problem.	[None]
114673-01	**wall** patch. Fixes vulnerability.	[None]
114986-01	**rpc.rexd** patch. Fixes denial of service vulnerability.	[None]
115797-01	**dtspcd** patch. Fixes memory leak problem	[None]
115823-01	**logger** patch. Fixes buffer overflow	[None]
116455-01	**sadmind** patch. Fixes vulnerability	[None]
Bugs: 2126267, 6248413, 4765506, 4805635, 4830406, 4913437, 4981868, 5007891, 5014993, 5044522	Fixes to various NIS+ vulnerabilities	[None]
Bug 4705157	**in.rwhod** patch. Fixes input validation vulnerability	[None]
Bug 4705393	Fix to buffer overflow in **newgrp**	[None]
Bugs 4786448, 4917860, 6182042, 6182042	CDE library fixes (segmentation faults, buffer overflows)	[None]
Bug 6234932	Fix to buffer overflow in **telnet** command	[None]

Table 8: Summary of TSP-Supporting Base Solaris Changes

Base Solaris Changes affecting Security Irrelevant Code

27. The following table provides a summary of changes to security irrelevant code in Base Solaris 8, i.e. those that do not affect any TSP-critical or TSP-supporting code. These include changes to features that are not within the scope of the evaluated configuration.

Item (Patch ID)	Description of change	Related changes
108434-13, 108435-29, 108962-01, 108977-02, 108995-06, 109043-02, 109244-02, 109384-07, 109529-06, 109607-02, 109873-24, 109881-02, 110385-04, 110605-02, 110611-01, 110716-02, 110724-01, 110811-01, 110813-01, 110815-01, 110817-01, 110912-04, 110939-01, 110941-03, 111098-01, 111225-02, 111562-02, 111721-04, 111802-02, 112989-01, 114160-01, 114610-01, 114982-01, 115579-01, 115583-01, 115829-01, 115831-01	Patches to security irrelevant library functions	[None]
108569-08, 110370-03, 110376-01, 110830-02, 110833-01, 110853-02, 110856-01, 111792-10, 111794-03, 111808-02, 111822-02, 112137-02, 112160-01, 112161-02, 112167-01, 112187-01, 113684-04, 116038-01, 116604-01, 116605-01	Security irrelevant updates to provide support for new hardwar e	[None]
108909-13, 108914-02, 108925-10, 109223-03, 109264-01, 109679-01, 109695-03, 109805-17, 109887-17, 109889-07, 110068-02, 110286-11, 110388-01, 110457-05, 112237-08 Bug 5055875	Fixes to bugs in features that are not in the scope of the evaluation (e.g. smartcard support, Apache)	[None]

Item (Patch ID)	Description of change	Related changes
108623-03, 108711-04, 108712-01, 108734-02, 108735-03, 108773-18, 108781-02, 108933-01, 108954-02, 108956-01, 109068-01, 109070-05, 109072-08, 109093-11, 109094-01, 109128-01, 109131-10, 109133-02, 109157-20, 109159-03, 109176-05, 109179-04, 109200-02, 109247-01, 109249-01, 109255-01, 109318-33, 109411-02, 109452-01, 109470-02, 109552-01, 109564-01, 109609-01, 109622-01, 109639-02, 109692-03, 109704-03, 109750-03, 109755-01, 109766-02, 109778-13, 109809-01, 109868-05, 109910-01, 109936-01, 109960-01, 109992-01, 110019-06, 110044-01, 110053-02, 110065-01, 110206-01, 110251-01, 110274-03, 110394-01, 110418-01, 110428-01, 110503-01, 110745-01, 110754-03, 110756-02, 110758-02, 110764-03, 110766-03, 110797-02, 110885-01, 110888-01, 110927-01, 111008-06, 111075-02, 111275-01, 111368-01, 111386-01, 111471-05, 111755-02, 111823-01, 111876-01, 111953-01, 112003-03, 112032-02, 112036-02, 112057-01, 112082-02, 112084-01, 112109-01, 112142-01, 112144-01, 112183-03, 112223-01, 112394-01, 112472-01, 113261-02, 113401-01, 114059-02, 114152-01, 114246-01, 114508-01, 114559-01, 114882-01, 115383-02	Problems with non-English or extended character input, display or translation issues, and localisation updates.	[None]

Item (Patch ID)	Description of change	Related changes
109003-01, 109009-02, 109011-01, 109013-02, 109015-01, 109017-01, 109019-02, 109021-01, 109023-02, 109025-04, 109027-01, 109029-02, 109031-01, 109033-01, 109037-01, 109087-01, 109165-13, 109167-01, 109169-12, 109441-05, 109463-01, 109568-03, 109569-01, 109573-01, 109613-06, 109642-01, 109748-03, 109752-01, 109785-01, 109803-01, 109807-01, 109813-01, 109877-01, 109890-01, 109931-06, 109990-01, 109994-02, 110165-04, 110326-02, 110335-02, 110364-02, 110381-01, 110407-02, 110603-01, 110609-04, 110662-12, 110752-01, 110864-01, 110905-02, 110907-01, 110914-01, 110916-04, 110986-02, 111016-01, 111073-01, 111111-03, 111141-03, 111231-04, 111265-01, 111295-01, 111297-01, 111313-01, 111319-01, 111323-01, 111398-01, 111481-01, 111760-02, 111775-01, 111777-01, 111800-01, 111844-02, 111958-02, 111989-01, 112050-02, 112138-01, 112165-01, 112171-01, 112274-02, 112328-02, 112345-03, 112371-01, 112396-02, 112597-02, 112663-01, 112666-01, 112670-01, 112781-01, 112844-02, 113128-02, 113372-02, 113413-01, 113415-01, 113417-01, 113419-01, 114155-02, 114158-01, 113364-01, 114512-02, 114667-01, 114773-01, 114802-01, 114988-02, 114990-02, 115274-02, 115795-01, 115825-01, 116332-01, 116602-01	Fixes to various bugs in security irrelevant commands or features.	[None]

Table 9: Summary of Security Irrelevant Changes to Base Solaris Code

Changes to Developer Evidence

28. Changes to the Security Target [c] are limited to changes to the TOE version number and the range of platforms claimed for Trusted Solaris 8.

29. There are no changes to the High Level Design, other than minor generic changes. Changes to the Low Level Design, test documentation and Developer Vulnerability Analysis have been listed above in the descriptions of the individual changes. The changes to the Developer Vulnerability Analysis involved minor updates where specific bug fixes have reduced the opportunities of an attacker with respect to known (but non-exploitable) vulnerabilities in Trusted Solaris 8 4/01.

30. Installation and guidance documentation has been updated to reflect the changes made to the product and its method of secure use, as indicated in the tables above and as summarised below under 'Installation and Guidance Documentation'.

31. There have been no changes to the Delivery Procedures.

32. The Multi-Platform Rationale has also been updated to cover the hardware platforms. The latest version covered by the updated rationale is Trusted Solaris 8 HW 7/03. The IAR [f] describes how this rationale applies equally to the range of platforms claimed for Trusted Solaris 8 2/04.

33. There have been no changes to other TOE documentation.

TOE Identification

34. The maintained TOE is uniquely identified as:

Trusted Solaris 8 2/04

35. Both software and documentation components of the maintained TOE (referred to as the *Certified Release*) are identified as follows:

- For SPARC platforms:

  CD Part Nos. 705-1372-10 and 705-1373-10, 2005

- For Intel and AMD platforms:

  CD Part Nos. 705-1374-10 and 705-1375-10, 2005

36. The Trusted Solaris 8 2/04 AnswerBook CD is:

CD Part No. 705-0926-10, 2005.

Installation and Guidance Documentation

37. The following documents have been updated. Both are included on the AnswerBook CD-ROM specified above under 'TOE Identification':

- Trusted Solaris 8 2/04 Release Notes,
  Part number 819-2258-10, dated 2005
  (updated for Trusted Solaris 8 2/04).

- Trusted Solaris 8 2/04 Transition Guide,
  Part number 817-3930-10, dated 2005

(outlining differences which Trusted Solaris 8 2/04 exhibits compared with each of Trusted Solaris 8 4/01, Trusted Solaris 8 HW 12/02 and Trusted Solaris 8 HW 7/03).

38. The Trusted Solaris 8 4/01 versions of other installation and guidance documents, specified in the Trusted Solaris 8 4/01 Certification Report [a] remain current for Trusted Solaris 8 2/04, with the exception of the following documents which have been updated:

- The Trusted Solaris 8 HW 12/02 roadmap remains current for Trusted Solaris 8 2/04 (when interpreted as referencing the above Trusted Solaris 8 2/04 documentation where references to equivalent Trusted Solaris 8 HW 12/02 documentation are made).
- Manual Pages — Some online man pages are new; others are updated on the online man command. These are all identified in Table 4 above. The reference manuals (volumes 1-9F) themselves have not been updated since the Trusted Solaris 8 HW 12/02 version, as the minor nature of the changes has not warranted republishing of the manuals.

Testing and Hardware Platforms

39. The Developer's testing was performed using both an automated test suite and additional manual tests. These tests included:

- The automated test suite run by the Developer for the Trusted Solaris 8 4/01 evaluation;
- The manual tests performed by the Developer for the Trusted Solaris 8 4/01 evaluation; and
- The additional functional tests and penetration tests performed by the Evaluators for the Trusted Solaris 8 4/01 evaluation.

40. The automated test suite was run on each of the platforms listed in Table 10 below. A sample of the manual tests (described in second and third bullets at paragraph 39 above) was run on each of the platforms listed in Table 10. The precise sample size varied but, on each platform, at least 60% of the manual functional tests, and at least 70% of the penetration tests, were run.

41. In addition to the above testing performed in respect of Trusted Solaris 8 2/04, the Developer had previously performed tests formulated to specifically check patches issued ahead of, and subsequently rolled into, this version. This was not considered to be part of the formal test evidence required for EAL4 Assurance Continuity, but served to provide sufficient confidence that the patches would be effective across the range of platforms claimed, without requiring testing on more than one platform.

42. To reproduce the pattern of usage which might typically be encountered on the more powerful platforms:

- The Developer also used a stress test suite, simulating a large number of login sessions, on the platforms marked with note (S) in the table below. The automated test suite was run both alone and concurrently with the stress test suite, on these platforms, to give confidence that the security functionality continued to operate as claimed under high load conditions.
- The Developer also used a race condition test suite, invoking multiple execution threads (e.g. for credential checking and file access), on the platforms marked with note (R) in the table below. Two copies of the race condition test suite were run concurrently with both the automated test suite and two copies of the stress test suite, to give confidence that no anomalies occurred in the behaviour of security functionality.

43. The single processor AMD Athlon machine was used as NFS server and NIS+ master wherever such functionality was required.

44. Whilst the Open Boot PROMs (OBPs), System Controller (SC) boards, OpenBoot PROM System Controller (OBPSC) boards and PC BIOS were in the environment of the TOE specified by the Security Target [c], some of the penetration tests investigated the security of the bootstrapping capability of the OBPs, SC boards and OBPSC boards on the SPARC platforms.

45. The environment of use specified by the Security Target [c] applied equally to the two laptop platforms.

46. Note that

a) Whilst some of the platforms included in the table below are no longer marketed, they featured in the Developer testing programme as some existing consumers with this hardware have upgraded or intend to upgrade their software to Trusted Solaris 8 2/04.

b) The terms UltraSPARC III and UltraSPARC IV are used generically, although a 1.2 GHz UltraSPARC III CPU is commonly known as an UltraSPARC III+ CPU and a 1.5 GHz UltraSPARC IV CPU is commonly known as an UltraSPARC IV+ CPU.

Platform	Processor and Memory	Hard Drive	SPARC Boot option	Notes (para 42)
SunBlade 1500	1062 MHz UltraSPARC III cpu, 1024 Mb memory	75 Gb	OBP v4.9.4	
SunBlade 2000	2 x 900 MHz UltraSPARC III cpu, 2048 Mb memory	73 Gb	OBP v4.5.16	
SunBlade 2500	2 x 1280 MHz UltraSPARC IIIi cpu, 4096 Mb memory	36 Gb	OBP v4.9.4	
ServerBlade 1	650 MHz UltraSPARC IIIi cpu, 512 Mb memory	30 Gb	OBP v4.7.5	

Platform	Processor and Memory	Hard Drive	SPARC Boot option	Notes (para 42)
SunFire V210	2 x 1002 MHz UltraSPARC IIIi cpu, 1024 Mb memory	2 x 36 Gb	OBP v4.8.2	
SunFire V240	2 x 1280 MHz UltraSPARC IIIi cpu, 2048 Mb memory	2 x 36 Gb	OBP v4.8.2	
SunFire V250	2 x 1280 MHz UltraSPARC IIIi cpu, 2048 Mb memory	4 x 36 Gb	OBP v4.11.4	
SunFire V440 Configuration 1	1 board, comprising: 1281 MHz UltraSPARC IIIi cpu, 2 Gb memory	4 x 36 Gb	OBP v4.10.1	
SunFire V440 Configuration 2	1 board, comprising: 1281 MHz UltraSPARC IIIi cpu, 2 Gb memory and 1 board, comprising: 1281 MHz UltraSPARC IIIi cpu, 4 Gb memory	4 x 36 Gb	OBP v4.10.1	
SunFire V440 Configuration 3	4 boards, each comprising: 1281 MHz UltraSPARC IIIi cpu, 4 Gb memory	4 x 36 Gb	OBP v4.10.1	
SunFire V480 Configuration 1	1 board, comprising: 2 x 900 MHz UltraSPARC III cpu, 2 Gb memory	2 x 36 Gb	OBP v4.6.4	
SunFire V480 Configuration 2	2 boards, each comprising: 2 x 900 MHz UltraSPARC III cpu, 2 Gb memory	2 x 36 Gb	OBP v4.6.4	
SunFire V490 Configuration 1	1 board, comprising: 2 x 1.05 GHz UltraSPARC IV cpu, 8 Gb memory and 1 board, comprising: 2 x 1.05 GHz UltraSPARC IV cpu, 16 Gb memory	2 x 146 Gb	OBP v4.15.1	(S), (R)
SunFire V490 Configuration 2	1 board, comprising: 2 x 1.05 GHz UltraSPARC IV cpu, 16Gb memory	2 x 146 Gb	OBP v4.15.1	(S)
SunFire V880 Configuration 1	1 board, comprising: 2 x 900 MHz UltraSPARC III cpu, 2 Gb memory	6 x 73 Gb	OBP v4.6.3	
SunFire V880 Configuration 2	2 boards, each comprising: 2 x 900 MHz UltraSPARC III cpu, 1 Gb memory	6 x 73 Gb	OBP v4.6.3	
SunFire V880 Configuration 3	2 boards, each comprising: 2 x 900 MHz UltraSPARC III cpu, 2 Gb memory	6 x 73 Gb	OBP v4.6.3	
SunFire V890 Configuration 1	4 boards, each comprising: 2 x 1.35 GHz UltraSPARC IV cpu, 16 Gb memory	6 x 146 Gb	OBP v4.15.6	(S)
SunFire V890 Configuration 2	2 boards, each comprising: 2 x 1.35 GHz UltraSPARC IV cpu, 16 Gb	6 x 146 Gb	OBP v4.15.6	(S)

Platform	Processor and Memory	Hard Drive	SPARC Boot option	Notes (para 42)
	memory			
SunFire V890 Configuration 3	1 board, comprising: 2 x 1.35 GHz UltraSPARC IV cpu, 16 Gb memory	6 x 146 Gb	OBP v4.15.6	(S), (R)
SunFire V1280	4 x 900 MHz UltraSPARC III cpu, 8192 Mb memory	2 x 36 Gb	SC v5.13.0009 (with RTOS v23)	
SunFire 2900 Configuration 1	1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	2 x 146 Gb	OBP v5.19.3	(S)
SunFire 2900 Configuration 2	2 boards, each comprising: 4 x 1.2 GHz UltraSPARC III cpu, 8 Gb memory and 1 board comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	2 x 146 Gb	OBP v5.19.3	(S)
SunFire 2900 Configuration 3	1 board, comprising: 4 x 1.2 GHz UltraSPARC III cpu, 8 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	2 x 146 Gb	OBP v5.19.3	(S), (R)
SunFire 3800 Configuration 1	1 board, comprising: 4 x 750 MHz UltraSPARC III cpu, 4 Gb memory	2 x 9 Gb	SC v5.13.2 (with RTOS v23)	(S), (R)
SunFire 3800 Configuration 2	1 board, comprising: 4 x 900MHz UltraSPARC III cpu, 8 Gb memory	2 x 9 Gb	SC v5.13.2 (with RTOS v23)	
SunFire 4900 Configuration 1	3 boards, each comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP v5.18.0	
SunFire 4900 Configuration 2	1 board, comprising: 2 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 8 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP v5.18.0	
SunFire 4900 Configuration 3	1 board, comprising: 2 x 1.2 GHz UltraSPARC IV cpu, 2 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP v5.18.0	
SunFire 6900 Configuration 1	1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 5.18.2	(S)

Platform	Processor and Memory	Hard Drive	SPARC Boot option	Notes (para 42)
SunFire 6900 Configuration 2	1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 8 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 5.18.2	(S)
SunFire 6900 Configuration 3	6 boards, each comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 5.18.2	(S)
SunFire 6900 Configuration 4	1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory and 1 board, comprising: 2 x 1.2 GHz UltraSPARC III cpu, 4 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC III cpu, 8 Gb memory 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 5.18.2	(S), (R)
SunFire 15K Configuration 1	1 board comprising: 4 x 1050MHz UltraSPARC III cpu, 4 Gb memory	8 x 80 Gb	SC OBP v3.1.4.6 (with Sol 8 10/01)	
SunFire 15K Configuration 2	1 board comprising: 2 x 1050MHz UltraSPARC III cpu, 4 Gb memory and 1 board comprising: 4 x 1050MHz UltraSPARC III cpu, 4 Gb memory and 2 boards, each comprising: 4 x 1050MHz UltraSPARC III cpu, 8 Gb memory and 1 board comprising: 4 x 1050MHz UltraSPARC III cpu, 16 Gb memory	8 x 80 Gb	SC OBP v3.1.4.6 (with Sol 8 10/01)	

Platform	Processor and Memory	Hard Drive	SPARC Boot option	Notes (para 42)
SunFire 15K Configuration 3	1 board comprising: 4 x 1050MHz UltraSPARC III cpu, 4 Gb memory and 1 board comprising: 4 x 1050MHz UltraSPARC III cpu, 8 Gb memory and 7 boards, each comprising: 4 x 1050MHz UltraSPARC III cpu, 16 Gb memory	8 x 80 Gb	SC OBP v3.1.4.6 (with Sol 8 10/01)	(S)
SunFire 15K Configuration 4	10 boards, each comprising: 4 x 1050MHz UltraSPARC III cpu, 4 Gb memory and 1 board comprising: 4 x 1050MHz UltraSPARC III cpu, 8 Gb memory and 2 boards, each comprising: 4 x 1050MHz UltraSPARC III cpu, 16 Gb memory and 1 MaxCPU processor board comprising: 2 x 1050MHz UltraSPARC III cpu	8 x 80 Gb	SC OBP v3.1.4.6 (with Sol 8 10/01)	
SunFire 15K Configuration 5	17 boards, each comprising: 4 x 1050MHz UltraSPARC III cpu, 16 Gb memory	8 x 80 Gb	SC OBP v3.1.4.6 (with Sol 8 10/01)	(S)
SunFire 20K Configurations 1 to 3	*Same specification as that below for SunFire 25K Configurations 1 to 3*			
SunFire 25K Configuration 1	1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 4.15.8	(S)
SunFire 25K Configuration 2	1 board, comprising: 2 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory and 2 boards, each comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 8 Gb memory 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 4.15.8	(S)

Platform	Processor and Memory	Hard Drive	SPARC Boot option	Notes (para 42)
SunFire 25K Configuration 3	1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 4 Gb memory and 1 board, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 8 Gb memory and 7 boards, comprising: 4 x 1.2 GHz UltraSPARC IV cpu, 16 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 4.15.8	(S), (R)
SunFire 25K Configuration 4	10 boards, comprising: 4 x 1.05 GHz UltraSPARC IV cpu, 8 Gb memory and 2 boards, comprising: 4 x 1.05 GHz UltraSPARC IV cpu, 16 Gb memory and 2 boards, comprising: 4 x 1.05 GHz UltraSPARC IV cpu, 32 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 4.13.3	(S)
SunFire 25K Configuration 5	18 boards, each comprising: 4 x 1.05 GHz UltraSPARC IV cpu, 32 Gb memory	1 x D240 Media Tray (DVD-ROM and 4 x146 Gb)	OBP 4.13.3	(S)
Intel P4	2.4 GHz Intel Pentium P4 cpu, 512 Mb memory	60 Gb	-	
Sony Vaio laptop	2498 MHz Intel Pentium P4 cpu, 512 Mb memory	15 Gb	-	
Panasonic laptop	1999 MHz Intel Pentium P4 cpu, 768 Mb memory	20 Gb	-	
Intel Xeon	2 x 24 GHz Intel Xeon cpu, 1024 Mb memory	60 Gb	-	
Netframe 1610 (SunFire V60)	2 x 3331 MHz hyperthreaded Intel Xeon cpu, 1024 Mb memory	2 x 18 Gb	-	(R)
Dell Poweredge 2650	2 x 3331 MHz Intel Xeon cpu, 1024 Mb memory	2 x 36 Gb	-	
AMD Athlon	2.4 GHz AMD Athlon cpu, 512 Mb memory	60 Gb	-	
AMD Athlon	2 x 2200 MHz AMD Athlon cpu, 512 Mb memory	60 Gb	-	
AMD Opteron	2 x 1.4 GHz AMD Opteron cpu, 2048 Mb memory	2 x 38 Gb	-	

Table 10: TSol8 2/04 Test Platforms

47. The Developer additionally performed multi-platform analyses to demonstrate that the relevant machines above were representative of the families given in Table 11 below, with respect to the claims of the Security Target [c] for the operation of Trusted Solaris 8 2/04 on such hardware platforms.

48. Note that a minimum memory of 256 Mb (to support administrator SMC requests on NFS server, NIS+ master workstations) or 128 Mb (on client workstations) and a minimum hard disk size of 2 Gb are recommended. There is a risk (which is more significant nearer these limits) that lower processor speeds, memory sizes or hard disk sizes than those tested may introduce performance degradation problems.[1]

Family	Processor Options	Memory Options	Hard Drive Options
SunFire V440	From 1 to 4 boards, each comprising: 1062MHz or 1280MHz UltraSPARC IIIi cpu	From recommended minimum to 32 Gb	From recommended minimum to 146 Gb
SunFire V480	1 or 2 boards, each comprising: 1 or 2 x 900, 1050 or 1200MHz UltraSPARC III cpu	From recommended minimum to 32 Gb	From recommended minimum to 146 Gb
SunFire V490	1 or 2 boards, each comprising: 1 to 4 x 1.05, 1.35 or 1.5 GHz UltraSPARC IV cpu (total 4 CPUs maximum)	From recommended minimum to 32 Gb	From recommended minimum to 292 Gb
SunFire V880	1 or 2 boards, each comprising: from 1 to 4 x 750, 900, 1050 or 1200 MHz UltraSPARC III cpu	From recommended minimum to 64 Gb	From recommended minimum to 876 Gb
SunFire V890	1 to 4 boards, each comprising: from 1 to 8 x 1.35, 1.5 GHz UltraSPARC IV cpu (total 8 CPUs maximum)	From recommended minimum to 64 Gb	From recommended minimum to 1.75 Tb

SunFire 2900	1 to 3 boards, each comprising:
	from 1 to 4 x 900, 1050 or 1200 MHz UltraSPARC III cpu, or
	from 1 to 4 x 1.05, 1.2, 1.35 or 1.5 GHz UltraSPARC IV cpu
	(total 12 CPUs maximum)
		From recommended minimum
		to 96 Gb
			From recommended minimum
			to 2 x 146 Gb internal (and external storage arrays available)

SunFire 3800	1 or 2 boards, each comprising: from 1 to 4 x 750, 900, 1050 or 1200 MHz UltraSPARC III cpu	From recommended minimum to 64 Gb	From recommended minimum to 35 Tb
SunFire 4900	1 to 3 boards, each comprising: from 1 to 4 x 1.05, 1.2, 1.35 or 1.5 GHz UltraSPARC IV cpu (total 12 CPUs maximum)	From recommended minimum to 96 GB	From recommended minimum StorEdge D240 Media Tray (4 x 146GB disks) to StorEdge 9000 series (330TB capacity)

[1] For the more powerful machines however, it is expected that significantly greater memory sizes and hard disk sizes will be used.

Family	Processor Options	Memory Options	Hard Drive Options

SunFire 6900	1 to 6 boards, each comprising:
	from 1 to 4 x 900, 1050 or 1200 MHz UltraSPARC III cpu, or
	from 1 to 4 x 1.05, 1.2, 1.35 or 1.5 GHz UltraSPARC IV cpu
	(total 24 CPUs maximum)
		From recommended minimum
		to 192 GB
			From recommended minimum
			StorEdge D240 Media Tray (4 x 146GB disks)
			to StorEdge 9000 series (330TB capacity)

SunFire 15K	From 1 to 18 system boards and, optionally, from 1 to 17 MaxCPU boards, each comprising: from 1 to 4 (system board) or 1 or 2 (MaxCPU board) 750, 900, 1050 or 1200 MHz UltraSPARC III cpu	From recommended minimum to 576 Gb	From recommended minimum to maximum permitted by disk array
SunFire 20K	From 1 to 9 system boards, each comprising: from 1 to 4 x 1.05, 1.2, 1.35 or 1.5 GHz UltraSPARC IV cpu (total 36 CPUs on Uniboards)	From recommended minimum to 288 GB	From recommended minimum to maximum permitted by disk array
SunFire 25K	From 1 to 18 system boards each comprising: from 1 to 4 x 1.05, 1.2, 1.35 or 1.5 GHz UltraSPARC IV cpu (total 72 CPUs on Uniboards)	From recommended minimum to 576 GB	From recommended minimum to maximum permitted by disk array

Table 11: TSol8 2/04 Platform Ranges Covered By Analysis

(This page is intentionally left blank)