National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Red Hat Enterprise Linux

AS Version 4 Update 4 with capp-eal3-config-sgi package

Report Number: CCEVS-VR-06-0035
Dated: 22 September 2006
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Executive Summary

This report documents the National Information Assurance Partnership (NIAP) Validator's assessment of the Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation of the Red Hat Enterprise Linux (RHEL) AS Version 4 Update 4.

The evaluation for RHEL AS Version 4 Update 4 was performed by atsec information security Common Criteria Testing Laboratory (CCTL) in the United States and was completed on 15 September 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3; Evaluation Assurance Level 3 (EAL3) augmented by ALC_FLR.3; and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.3.

The TOE meets the requirements of the Controlled Access Protection Profile (CAPP) developed by the Information Systems Security Organization within the National Security Agency to map the Trusted Computer System Evaluation Criteria (TCSEC) C2 class of the U.S. Department of Defense (DoD) to the Common Criteria framework. Therefore, full compliance is claimed with the requirements of this Protection Profile; also, additional functional and assurance packages beyond those required by CAPP have been included.

The evaluation covers a potentially distributed, but closed network of Silicon Graphics, Inc. (SGI) Altix servers running the evaluated version of Red Hat Enterprise Linux. Several servers running Red Hat Enterprise Linux can be connected to form a networked system. The communication aspects within Red Hat Enterprise Linux used for this connection are also part of the evaluation. Communication links can be protected against loss of confidentiality and integrity by security functions of the TOE based on cryptographic protection mechanisms. Since this evaluation focuses on the use of the TOE as a server or a network of servers, a graphical user interface has not been included as part of the evaluation. In addition, the evaluation assumes the operation of the network of servers in a non-hostile environment. The TOE includes the hardware and firmware used to run the software components.

The TOE provides the following seven security features, which are described in greater detail in Section 3 of this report:

1. Identification and Authentication
2. Security Audit
3. Discretionary Access Control
4. Object Reuse Functionality
5. Security Management
6. Secure Communication
7. TSF Protection

atsec information security is an approved National Information Assurance Partnership (NIAP) CCTL. The CCTL concluded that the Common Criteria assurance requirements for EAL 3+ have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of the RHEL AS Version 4 Update 4 by any agency of the US Government and no warranty of the product is either expressed or implied.

Table ES-1 provides the required evaluation identification details.

Table ES-1. Evaluation Details

Item	Description
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	Red Hat Enterprise Linux AS Version 4 Update 4
EAL	EAL3+
Protection Profile	CAPP
Security Target	Red Hat Enterprise Linux AS Version 4 Update 4 Security Target for CAPP Compliance Version 2.8, dated 22 August 2006
Developer	Red Hat, Inc.
Sponsor	Silicon Graphics, Inc. (SGI)
Evaluators	Stephan Mueller, Lead Evaluator Fiona Pattinson, Lab Manager atsec information security; Austin, TX
Validator	Catalina M. Gomolka Mitretek Systems; Falls Church, VA
Dates of Evaluation	July 2006 to September 2006
Conformance Result	Part 2 extended and Part 3 conformant, with a claimed Evaluation Assurance Level of EAL3 augmented by ALC_FLR.3
Common Criteria (CC) Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, Part 1 to 3
Common Evaluation Methodology (CEM) Version	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation Red Hat Enterprise Linux Version 4 Update 4 AS Red Hat Enterprise Linux Version 4 Update 4 Security Target for CAPP compliance, version 2.8, 2006-08-22 claiming compliance with Controlled Access Protection Profile, Issue 1.d, 8 October 1999 Version 1.0, 2006-09-15

Table of Contents

Table of Tables and Figures

Table of Figures

1 Identification of the TOE

The Target of Evaluation (TOE) is the operating system Red Hat Enterprise Linux (RHEL) AS Version 4 Update 4 with the capp-eal3-config-sgi package. It is a Linux based multi-user multi-tasking operating system. The TOE meets the requirements of the Controlled Access Protection Profile (CAPP) developed by the Information Systems Security Organization within the National Security Agency to map the Trusted Computer System Evaluation Criteria (TCSEC) C2 class of the U.S. Department of Defense (DoD) to the Common Criteria framework. Therefore, full compliance is claimed with the requirements of this Protection Profile; also, additional functional and assurance packages beyond those required by CAPP have been included.

The evaluation covers a potentially distributed, but closed network of Silicon Graphics, Inc. (SGI) Altix servers running the evaluated version of Red Hat Enterprise Linux. Several servers running Red Hat Enterprise Linux can be connected to form a networked system. The communication aspects within Red Hat Enterprise Linux used for this connection are also part of the evaluation. Communication links can be protected against loss of confidentiality and integrity by security functions of the TOE based on cryptographic protection mechanisms. Since this evaluation focuses on the use of the TOE as a server or a network of servers, a graphical user interface has not been included as part of the evaluation. In addition the evaluation assumes the operation of the network of servers in a non-hostile environment. The TOE includes the hardware and firmware used to run the software components.

The TOE Security Functions (TSF) consist of operating system functions that run in kernel mode plus some trusted processes. These are the functions that enforce the security policy as defined in the Security Target. Tools and commands executed in user mode that are used by an administrative user also need to be trusted to manage the system in a secure way. The basic tools required for the secure configuration and management of the TOE have been included as part of the TSF in this evaluation.

The TOE provides a general computing environment, allowing the startup of user applications, issuing user commands at shell level, creating and accessing files after a successful login. The TOE provides adequate mechanisms to separate the users and protect their data. Privileged commands are restricted to administrative users. The TOE uses the standard UNIX model of normal (unprivileged) users and administrative users that have the capability to get full root privileges. The TOE permits one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled shared access to the data stored on the system. It is assumed that responsibility for the safeguarding of the data protected by the TOE can be delegated to the TOE users. All data is under the control of the TOE. The data is stored in named objects, and the TOE can associate with each named object a description of the access rights to that object. All individual users are assigned a unique user identifier within the single host system that forms the TOE. This user identifier is used as the basis for access control decisions. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions. The TOE enforces controls such that access to data objects can only take place in accordance with the access restrictions placed on that object by its owner or administrative users. Ownership of named objects may be transferred under the control of the access control policy.

Access rights (e.g. read, write, execute) can be assigned to data objects with respect to subjects (users). Once a subject is granted access to an object, the content of that object may be freely used to influence other objects accessible to this subject.

Red Hat Enterprise Linux has the following security extensions:

- Access Control Lists,
- A Journaling File System,
- Integrated authentication framework (Pluggable Authentication Module [PAM]),
- A dedicated auditing subsystem. This auditing subsystem allows for the auditing of security critical events and provides tools for the administrative user to configure the audit subsystem and evaluate the audit records.
- Basic hardware check functions. They allow an administrative user to check on demand if the basic security functions of the hardware the TOE relies upon are provided correctly.

2 Interpretations

The Evaluation Team performed an analysis of the international and national interpretations of the CC and the CEM. The following interpretations applied:

- **National Interpretations**
  Final Interpretation for RI # 137 - Rules governing binding should be specifiable. Date: 1/30/2004

- **International Interpretations**
  Final Interpretation for RI # 86 - Role of Sponsor
  Final Interpretation for RI # 137 - Rules governing binding should be specifiable
  Final Interpretation for RI # 146 - C&P elements include characteristics
  Final Interpretation for RI # 175 - Circular Arguments in the objectives of FUN.2
  Final Interpretation for RI # 180 - COV.3 dependency on FSP.1
  Final Interpretation for RI # 192 - Sequencing of sub-activities
  Final Interpretation for RI # 220 - FCS_CKM/COP dependency on FDP_ITC.1
  Final Interpretation for RI # 227 - CC Part2 F.12 user notes
  Final Interpretation for RI # 228 - Inconsistency between FDP_ITC and FDP_ETC
  Final Interpretation for RI # 232 - FDP_ROL statement
  Final Interpretation for RI # 243 - Must Test Setup And Cleanup Code Run Unprivileged?
  Final Interpretation for RI # 254 - Applicability of ISO/IEC standards

3 Security Policy

The TOE provides the following seven security features:

1. Identification and Authentication
2. Security Audit
3. Discretionary Access Control
4. Object Reuse Functionality
5. Security Management
6. Secure Communication
7. TSF Protection

3.1 Identification and Authentication

The TOE provides identification and authentication using PAM based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by the TOE. Other authentication methods (e.g., Kerberos authentication, token based authentication) that are supported by the TOE as pluggable authentication modules are not part of the evaluated configuration. Functions to ensure medium password strength and limit the use of the *su* command and restrict root login to specific terminals are included.

3.2 Security Audit

The TOE provides an audit capability that allows generating audit records for security critical events. The administrative user can select which events are audited and for which users auditing is active. The TOE provides tools that help the administrative user extract specific types of audit events, audit events for specific users, audit events related to specific file system objects or audit events within a specific time frame from the overall audit records collected by the TOE. The system stores audit records in human-readable text format. The audit system detects when the capacity of the audit trail exceeds configurable thresholds, and the system administrator can define actions to be taken when the threshold is exceeded. The audit function also ensures that no audit records get lost due to exhaustion of the internal audit buffers. In the unlikely case of unrecoverable resource exhaustion, the kernel audit component can be configured to initiate a kernel panic to prevent all further auditable events.

3.3 Discretionary Access Control

Discretionary Access Control (DAC) restricts access to file system objects based on Access Control Lists (ACLs) that include the standard UNIX permissions for user, group and others. Access control mechanisms also protect interprocess communication (IPC) objects from unauthorized access. The TOE includes the ext3 file system, which supports POSIX ACLs. This allows defining access rights to files within this type of file system down to the granularity of a single user.

3.4 Object Reuse Functionality

File system objects as well as memory and IPC objects will be cleared before they can be reused by a process belonging to a different user.

3.5 Security Management

The management of the security critical parameters of the TOE is performed by administrative users. There is a set of commands that require root privileges, which are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users that are not administrative users.

3.6 Secure Communication

The TOE supports secure communication with other systems via the Secure Shell (SSH) v2 and Secure Socket Layer (SSL) v3 protocol. Communication via the SSH v2 and SSL v3 protocols is protected against unauthorized disclosure and modification via cryptographic mechanisms. The TOE also allows for secure authentication of the communicating parties using the SSL v3 protocol with client and server authentication. This allows establishing a secure communication channel between different machines running the TOE even over an insecure network. The SSL v3 protocol can be used to tunnel otherwise unprotected protocols in a way that allows an application to secure its transmission control protocol (TCP) based communication with other servers (provided the protocol uses a single TCP port).

3.7 TSF Protection

While in operation, the kernel software and data are protected by the hardware memory protection mechanisms. The memory and process management components of the kernel ensure a user process cannot access kernel storage or storage belonging to other processes. Non-kernel TSF software and data are protected by DAC and process isolation mechanisms. In the evaluated configuration, the reserved user ID root owns the directories and files that define the TSF configuration. In general, files and directories containing internal TSF data (e.g., configuration files, batch job queues) are also protected from reading by DAC permissions. The TOE including the hardware and firmware components are required to be physically protected from unauthorized access. The system kernel mediates all access to hardware components that are protected from direct access by user programs. A user process may execute unprivileged instructions and read or write to memory and processor register within the bounds defined by the kernel for the user process without those types of access being mediated by the kernel. All other types of access to hardware resources by user processes can only be performed by requests (in the form of system calls) to the kernel. The TOE provides a tool that allows an administrative user to check the correct operation of the underlying hardware. This tool performs tests to check the system memory, the memory protection features of the underlying processor and the correct separation between user and supervisor state.

4 Assumptions and Clarification of Scope

This section indicates the minimum physical and procedural measures required to maintain security of the TOE.

4.1 Assumptions

This section contains assumptions regarding the physical, personnel, and connectivity aspects for the intended usage of the TOE. Table 4-1 identifies the specific conditions that are assumed to exist in an environment where the TOE is employed.

Table 4-1. Assumptions

Physical Aspects		
1	A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
2	A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. **Application Note:** This includes the interfaces to and the L1/L2 controllers and all attached devices.
Personnel Aspects		
3	A.MANAGE	It is assumed that there are one or more competent individuals who are assigned to manage the TOE and the security of the information it contains.
4	A.NO_EVIL_ADMIN	The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
5	A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
6	A.UTRAIN	Users are trained to use the security functionality provided by the system appropriately.
7	A.UTRUST	Users are trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their data.
Connectivity Aspects		
8	A.NET_COMP	All network components (such as bridges and routers) are assumed to correctly pass data without modification.
9	A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. There are no security requirements which address the need to trust external systems or the communications links to such systems.
10	A.CONNECT	All connections to peripheral devices and all network connections not using the secured protocols SSH v2 or SSL v3 reside within the controlled access facilities. Internal communication paths to access points such as terminals or other systems are assumed to be adequately protected.

4.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed security threats are listed in Table 4-2.

Table 4-2. Threats

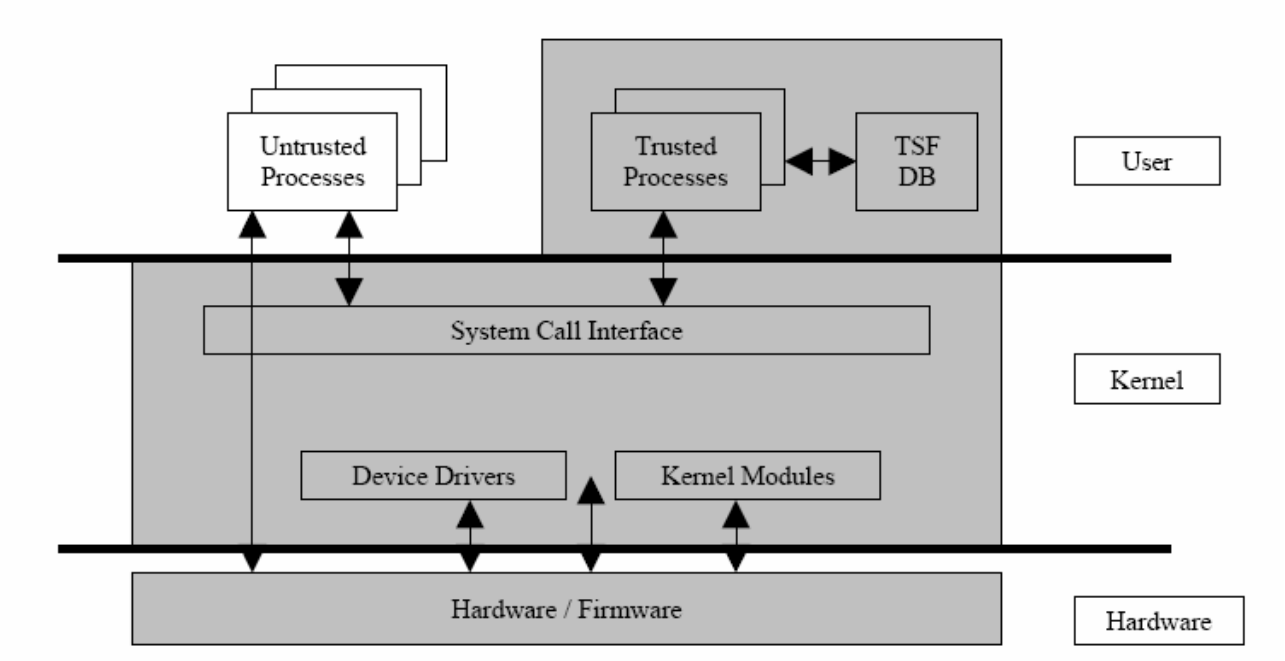
Threats countered by the TOE		
1	T.UAUSER	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) may impersonate an authorized user of the TOE. This includes the threat of an authorized user that tries to impersonate as another authorized user without knowing the authentication information.
2	T.UAACCESS	An authorized user of the TOE may access information resources without having permission from the person who owns, or is responsible for, the information resource for the type of access.
3	T.COMPROT	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) may intercept a communication link between the TOE and another trusted IT product to intercept or modify information transferred between the TOE and the other trusted IT product (which may be another instantiation of the TOE) using defined protocols (SSH or SSL) in a way that can not be detected by the TOE or the other trusted IT product.
Threats to be countered by measures within the TOE environment		
4	TE.HWMF	An attacker with legitimate physical access to the hardware of the TOE (examples are maintenance personnel or legitimate users) or environmental conditions may cause a hardware malfunction with the effect that a user (normal or administrative) is losing stored data due to this hardware malfunction. An attacker may cause such a hardware malfunction either by having physical access to the hardware the TOE is running on or by executing software that capable of causing hardware malfunction. Note that such a hardware malfunction may be caused accidentally without malicious intent by persons having physical access to the TOE.
5	TE.COR_FILE	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) or environmental conditions like a hardware malfunction may intentionally or accidentally modify or corrupt security enforcing or relevant files of the TOE without an administrative user being able to detect this. An attacker may corrupt such files either by having physical access to the hardware the TOE is running on, by booting other software than the TOE in its evaluated configuration or by modifying or corrupting files on backup media. Note that such a corruption may be caused accidentally without malicious intent by persons having legitimate access to media where such data is stored.

5 Architectural Information

The structure of the TOE consists of a kernel, which runs in the privileged state of the processor and provides services to applications. Direct access to the hardware is restricted to the kernel, so whenever an application wants to access hardware such as disk drives, network interfaces, or other peripheral devices, it has to call kernel services. The kernel then checks if the application has the required access rights and privileges and either performs the service or rejects the request. The kernel is also responsible to separate the different user processes. This is done by the management of the virtual and real memory of the TOE, which ensures that processes executing with different attributes can not directly access memory areas of other processes, but have to do so using the inter-process communication mechanism provided by the kernel as part of its system call interface. The TSF of the TOE also include a set of trusted processes, which when initiated by a user with a system call operate with extended privileges. The programs that represent those trusted processes on the file system are protected by the file system discretionary access control security function enforced by the kernel. In addition, the execution of the TOE is controlled by a set of configuration

files, which are also called the TSF database. Those configuration files are protected by the file system discretionary access control security function enforced by the kernel. Normal users – after successful authentication by a defined trusted process – can start untrusted applications where the kernel enforces the security policy of the TOE when those applications request services from the kernel via the system call interface. This structure is shown in Figure 5-1.

Figure 5-1. TOE Structure



The TOE comprises a single server machine (and optional peripherals) listed in section 5.1 running the system software listed in section 5.2.

5.1 Hardware

The hardware on which the software components of the TOE are executed is considered part of the TOE. The TOE consists of the TOE software running on an SGI ALTIX 4000 or 400 series server consisting of a combination of the following blade types:

- Compute/Memory blade
- Memory-only blade
- Base I/O Blade
- PCI-X expansion blade
- PCI-Express expansion blade

The hardware partition facility of Altix is not supported in the evaluated configuration and must not be used. RASC blades are also not supported in the evaluated configuration.

The following peripherals can be used with the TOE preserving the security functionality:

- All terminals supported by the TOE (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces).
- Printers compatible with PostScript level 1 or PCL 4 attached via parallel port, USB, or Ethernet.
- All storage devices and backup devices supported by the TOE (hard disks, CDROM drives, streamer drives, floppy disk drives) (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)
- All Ethernet and Token-Ring network adapters supported by the TOE

Note: Peripheral devices are part of the TOE environment.
Note: Excluding hot pluggable devices connected via USB does not exclude all USB devices. USB printers, keyboards and mice may be attached provided they are connected before booting the operating system.

5.2 Software

The Target of Evaluation system software consists of the Red Hat Enterprise Linux AS Version 4 Update 4 and the capp-eal3-config-sgi package. The TOE and its documentation are supplied on CD-ROM except for the capp-eal3-config-sgi package, which must be downloaded from Red Hat web site. This package contains the Evaluated Configuration Guide (ECG), which consists of all packages that have been updated to fix problems and scripts that can be used for the secure installation process. The user needs to verify the integrity and authenticity of those packages using the standard package verification procedure as described in the manuals distributed with the product.

Additionally, the Security Target for this evaluated product contains a full list of packages that make up the TOE in the evaluated configuration. This list includes packages that contribute to the TSF, as well as packages that contain untrusted user programs from the distribution.
(Note: Additional untrusted user programs may be installed and used as long as they are not *setuid* or *setgid* to root).

5.3 TOE Environment

Several TOE systems may be interlinked in a network, and individual networks may be joined by bridges and/or routers, or by TOE systems, which act as routers and/or gateways. Each of the TOE systems implements its own security policy. The TOE does not include any synchronization function for those policies. As a result, a single user may have user accounts on each of those systems with different user IDs, different roles, and other different attributes. (A synchronization method may optionally be used, but it not part of the TOE and must not use methods that conflict with the TOE requirements). If other systems are connected to a network they need to be configured and managed by the same authority using an appropriate security policy that does not conflict with the security policy of the TOE. All links between this network and untrusted networks (e.g., the Internet) need to be protected by appropriate measures, such as the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE, or including carefully configured firewall systems that prohibit attacks from the untrusted networks. Those protections are part of the TOE environment.

6 Documentation

The following is a list of the evaluation evidence used in the evaluation of the Red Hat Enterprise Linux AS Version 4 Update 4.

Reference	Document Title	Version	Date
ADMIN	Red Hat Enterprise Linux System Administration Guide rhel-sag-en.pdf	RHEL4	nil
AES	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) rfc3268.txt	nil	June 2002
BACKUP	RHEL Development Servers Backup Policy RHELBackupInfo.pdf	nil	2004-04-16
BEEHIVE	Red Hat - UsingBeehive UsingBeehive.pdf	nil	2005-03-24
BGGUIDE	Boston Office General Guidelines BostonGeneralGuidelines.pdf	nil	2004-04-14
BUILD	Using Internal Build System BuildSystemHOWTO.pdf	nil	2004-03-25
CVSBOOK	Open Source Development with CVS cvsbook.html	1.21	2005-03-24
CVSDEV	Red Hat - CvsDevel CvsDevel.pdf	nil	2004-03-25
CVSPP	CVS procedures and policies RHLPkgCVS.pdf	nil	2005-03-25
CVSSSH	Using CVS Without Passwords CVSandSSH.pdf	nil	2005-03-24
DELMGT	Red Hat Enterprise Linux Delivery Management Delivery_management_12b.pdf	2005.01.01	2003-10-29
DEVPOL	Code development policy CodevelopmentPolicy.pdf	nil	2004-04-16
DINTRO	Red Hat Product Engineering Introduction DevelIntro.pdf	nil	2005-03-24
ECG	Common Criteria EAL3+ Evaluated Configuration Guide for Red Hat Enterprise Linux on SGI Hardware RHEL-CAPP-EAL3-SGI-Configuration-Guide-v2.6.pdf	2.6	2006-08-15
EPP	Errata Policies & Processes ErrataProcess.pdf	nil	2004-04-13
ERRROT	Errata Rotation ErrataRotation.pdf	nil	2004-04-13
FSP	Archive with manual pages and auxiliary documentation as functional specification fsp-man-pages.tar.bz2	nil	nil
GGUIDE	General Guidelines GeneralGuidelines.pdf	nil	2004-03-25
HLD	Red Hat Enterprise Linux 4 Update 4 High Hevel Design SGI-RHEL4-HLD-v4.3.pdf	4.3	2006-08-04
IA64-1	Intel Itanium Architecture Software Developer's Manual - Volume 1 245317.pdf	Revision 2.1	October 2002

IA64-2	Intel Itanium Architecture Software Developer's Manual - Volume 2 245318.pdf	Revision 2.1	October 2002
IA64-3	Intel Itanium Architecture Software Developer's Manual - Volume 3 245319.pdf	Revision 2.1	October 2002
IDPOL	Identification Badge Policy IDBadgePolicy.pdf	nil	2004-03-25
IDREQ	Identification Badge Procedures IDBadgeProcedures.pdf	nil	2004-04-14
INSTALL	Installation Guide for x86, Itanium, AMD64, and Intel Extended Memory 64 Technology (Intel EM64T) rhel-ig-x8664-multi-en.pdf	RHEL4	nil
L1L2	SGI L1 and L2 Controller Software User's Guide 007-3938-003.pdf	003	May 2004
LCOVRES	LCOV test results lcov-out-2006-08-08.tar.bz2	nil	nil
QA	QA Errata Testplan QAErrataTestplan.pdf	nil	2004-04-13
REF-GUIDE	Reference Guide rhel-rg-en.pdf	RHEL4	nil
RHBUGZILLA	Screenshot of Bugzilla states rhbugzilla.pdf	nil	nil
RHERP	Red Hat Engineering review process EngReview-1.2.pdf	1.2	2004-07-26
RHNHWLIST	Screenshot from RHN listing the supported hardware platforms for RHEL rhnhwlist.pdf	nil	nil
RHNISO	Screenshot from RHN listing the ISO images for RHEL4 IA64 rhniso.pdf	nil	nil
RHNPKG	Screenshot from RHN listing the kernel package description for IA64 rhnpkg.pdf	nil	nil
RHNPREF	Red Hat Preferences rhnprefs.pdf	nil	nil
RHSA	RHSA checklist RHSAChecklist.pdf	nil	2003-03-25
RHSECTEAM	Red Hat security contacts rhsecteam.pdf	nil	nil
RHSLATIME	Red Hat SLA response times rhslatimes.pdf	nil	nil
SEC-GUIDE	Security Guide rhel-sg-en.pdf	RHEL4	nil
SGICM	SGI Configuration Management Plan sourceworks.pdf	1.2	nil
SOURCEWORKS	Introduction to SourceWorks SW_Intro.pdf	nil	2005-03-21
SRCLIST	Source code configuration list cvs-logs.tar.gz	nil	nil
SRP	Security Response Process SecurityResponseProcess.pdf	nil	nil

SSH	SSH Transport Layer Protocol rfc4253.txt	nil	January 2006
SSL	The SSL Protocol Version 3.0 draft302.txt	nil	1996-11-18
SSLCERT	SSL certificate verification of rhn.redhat.com sslcert.jpg	nil	2006-04-19
ST	Red Hat Enterprise Linux Version 4 Update 4 Security Target for CAPP compliance SGI-RHEL4_security_target_eal3-2.7.pdf	2.7	2006-08-11
STARTUP	Red Hat Enterprise Linux Step By Step Guide rhel-sbs-en.pdf	RHEL4	nil
TC	test case archive testcases.tar.gz	nil	nil
TCA	Evaluator test case analysis Testcaseanalysis.html	nil	nil
TDA	Test Depth Analysis for SLES9 SP2 with ProPack4 SP2 DPT-v1.0.html	1.0	2005-07-29
TESTCML	Evaluation specific documents configuration list sourceworks.log	nil	2006-08-11
TP	Test Plan for RedHat Enterprise Linux Version 4 - Update 4 (RHEL4-U4) EAL3 Security Function Verification RHEL4-CAPP-EAL3-SGI-Test_Plan.html	1.7	nil
TPE	Evaluator Test Plan for RHEL4 U4 EvaluatorTestPlan-1.0.pdf	1.0	2006-08-11
TRES	Developer test results RHEL4-developer-results.tar.gz	nil	2006-08-10
TRESE	Evaluator test results evaluator-testresults.tar.gz	nil	2006-08-11
VA	Vulnerability Assessment SGI-eal3-1.0.pdf	1.0	2006-08-12
WEBCM	Back Up Copies BackUpCopies.pdf	nil	2004-04-16
WLAN	Wireless Network Access In The Centennial Office wireless.pdf	nil	2004-04-14
XREF	SGI/Red Hat RHEL4U4 FSP Mapping Table fsp-sgi-v2.6.html	2.6	2006-08-09

7 IT Product Testing

7.1 Developer Testing

7.1.1 Test configuration

The test results provided by the sponsor were generated on the following system:

SGI Altix 4700:
128 Intel Itanium2 CPUs
128 GB RAM

The software was installed and configured as defined in the Evaluated Configuration Guide (ECG) with additional software packages identified in the Test Plan (TP). The Test Plan presents the arguments that those additional packages are within the boundary defined by the Security Target and do not constitute a violation of the evaluated configuration (see the chapter headed “Target of Evaluation (TOE) compliance” in [TP]).

7.1.2 Testing approach

The Test Plan provided by the sponsor lists test cases by groups, which reflects the mix of sources for the test cases. The mapping provided lists the TSF and TOE Security Functions Interface (TSFI) the test cases are associated with. The Test Plan focuses on the security functions of the TOE. The test cases are mapped to the corresponding functional specification and high-level design (HLD). The sponsor uses several test suites, which are integrated into one (automated) test system and manual tests to test the TOE. All the following discussed test suites are part of automated test cases.

The Linux Test Project (LTP) test suite is an adapted version of tests from the Linux Testing Project of which the sponsor is a member. The LTP tests have a common framework in which individual test cases adhere to a common structure for setup execution and cleanup of tests. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behavior with illegal parameters and reaction to missing privileges). Each test within a test case reports PASS respectively OK or FAIL and the test case summary in batch mode reports PASS if all the tests within the test case passed, otherwise FAIL. Tests can be executed either manually by running the test case file in the test cases/bin directory or run in batch mode by executing make run. This invokes a script that is controlled by various parameters. One of them (-l) specifies the log summary file for the test cases. If no parameters indicating the test cases to be run are given, the script uses a built-in list of test case lists to select the tests. Custom test case lists can be specified on the command line via the –f flag. When the test cases are run individually no log summary is generated. The user running the test cases has to inspect Standard Out and Standard Error of the process. The ‘at’ tests are simple expect scripts that execute one test per script and report PASSED or FAILED for each test case. A driver script (runme.sh) runs all the test cases and summarizes the PASSED / FAILED entries at the end.

For the ACL tests, the test cases contain comments, shell scripts, and expected output. The driver script for the test cases runs the shell commands and compares the output with the expected output in the test scripts. Each output line that matches is tagged with OK; each line that does not match is

tagged with FAILED. The driver scripts summarize the OK/FAILED entries and report the number of each of the two flags at the end. The test case reports 101 OK entries when executed successfully. The tests are started in batch mode via the runme shell script. The OpenSSL tests execute a part of the LTP OpenSSL test suite adapted for the security evaluation.

The audit tests use their own testing framework, where each test is executed up to eight times with varying goals. The tests iterate over the test with three parameters: system call success or failure, log entry, or no log entry. For each of the areas in the audit test suite, a driver program will perform global setup and run the individual test cases. Any FAIL entries are summarized by the calling Makefile.

The manual tests cover functionality that can not easily be tested in an automated way, such as console login. Appendix B in the Test Plan contains template text files that detail the exact steps required, along with the expected results. The tester creates a copy of the template, inserts the actual results, and compares them with the expected ones manually.

The cipher compliance tests were given to the developer by the evaluator and executed on the TOE. The test results were returned to the evaluator who validated their correctness. This testing is considered to be a special part of the overall testing and is therefore not included into the automated test suite.

All the sponsor tests were executed successfully (PASS/OK) apart from the test cases that are documented to fail or be skipped in the sponsor test plan. The test systems were configured according to the Security Target (ST) and the instructions in the ECG. The manual test results included in sponsor test plan also include PASS/FAIL labeling by the sponsor.

7.1.3 Testing results

The test results provided by the sponsor were generated on the hardware platforms listed above. As described in the testing approach, the test results of all the automated tests are written to files. In addition a log-file for the LTP tests reports more details on the flow of the tests. The test results of the few manual tests have been recorded by the sponsor and those results have been presented in separate files. All test results from all tested platforms show that the expected test results are identical to the actual test results, considering the expected failures stated in the test plan. The responses the evaluator retrieved from the developer for the cipher compliance testing were verified with the reference implementation provided with the CAVS FIPS 140-2 tool (for AES, 3DES, RSA, SHA) and ARCFOUR (for RC4). The validation of the developer’s cipher results with the reference implementation showed that all ciphers in the OpenSSL library of the TOE show consistent results with the reference implementations.

7.1.4 Test coverage

The functional specification has identified three different TSFI:

1. System calls,
2. Security critical configuration files (TSF databases), and
3. Trusted programs and the corresponding network protocols of SSHv2 and SSLv3.

A mapping provided by the sponsor shows that the tests cover all individual TSFI identified for the TOE. An extension to this mapping developed by the evaluators as documented in the test case coverage analysis document show that also significant details of the TSFI have been tested with the sponsor's test suite. This therefore satisfies the requirements for the evaluation, since an exhaustive specification testing is not required as outlined in CEM, paragraph 1062.

7.1.5 Test depth

In addition to the mapping to the functional specification, the sponsor provided a mapping of test cases to subsystems of the high level design. This mapping shows that all subsystems are covered by test cases. Using the high-level design, the coverage of internal interfaces was evident. To show evidence that the internal interfaces have been called, the sponsor provided the results of test cases that had been executed on a system installed and configured in compliance with the Security Target and the Evaluated Configuration Guide, but where large parts of the kernel had been compiled with the instrumentation for the gcov coverage analysis tool. This tool allows extracting a profile of all the source code statements that have been executed as part of the tests including numbers showing how often each source code statement has been executed. Part of the depth analysis was based on the output generated with those gcov instrumented kernels. Not all of the internal interfaces mentioned in the high level design could be covered by direct test cases. Some internal interfaces can – due to the restrictions of the evaluated configuration – only be invoked during system startup. This includes especially internal interfaces to load and unload kernel modules, to register/deregister device drivers and install/uninstall interrupt handler. Since the evaluated configuration does not allow dynamically loading and unloading device drivers as kernel modules, those interfaces are only used during system startup and are therefore implicitly tested there.

7.1.6 Conclusion

The evaluator has verified that developer testing was performed on hardware conformant to the ST. The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the sponsor. The evaluator analyzed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification. The evaluator reviewed the test results provided by the sponsor and found them to be consistent with the test plan. There were three test cases that showed a fail result during testing. The analysis showed that the affected functionality within the TOE is not security sensitive. Therefore, the developer chose to not immediately fix the issues.

7.2 Evaluator Testing

7.2.1 TOE test configuration

The evaluator independently installed the test systems according to the documentation in the ECG and the test plan. As assessed in the evaluation report on the administrator guidance, ECG is consistent with the ST. Hence, the evaluator concludes that the evaluator's configuration is consistent with the ST.

SGI Altix 4700:

The SGI Altix 4700 is located at the developer facility in Eagan, MN. The hardware configuration is equivalent to the system used by the sponsor to perform testing (see 3:ATE_FUN.1-12). The hardware consisted of the following types of blades:

Compute/Memory blade
Memory-only blade
Base I/O Blade
PCI-X expansion blade
PCI-Express expansion blade

7.2.2 Evaluator tests performed

In addition to repeating all the automated developer tests, the evaluator devised tests for a subset of the TOE. The tests are listed in the Evaluator Test Plan. The evaluator has chosen these tests for the following reasons:

- The test cases examine some of the security functions of the TOE in more detail than the sponsor supplied test cases. (Object reuse, Audit data protection records, password quality)
- The test cases cover aspects not included in the developer testing (verification of the long password support, verification of the ACL support in the archival tool, reaction to missing PAM configuration)

As the sponsor-supplied test cases already cover the TOE in a broad sense the evaluator has devised only a small set of test cases. The evaluator created several test cases for testing a few functional aspects where the sponsor test cases were not considered by the evaluator to be broad enough.

During the evaluator coverage analysis of the test cases provided by the sponsor, the evaluator gained confidence in the sponsor testing effort and the depth of test coverage in the sponsor supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the evaluator devised only a small number of test cases.

7.2.3 Summary of Evaluator test results

The evaluator testing effort consisted of two parts. The first one was the re-run of the developer test cases and the second was the execution of the tests created by the evaluator. The tests were performed at the sponsor's facility in Eagan, MN. In each case, the system was accessible through SSH and the system's consol exported by the L1/L2 firmware. The TOE operating system with the required additional RPM, as well as the test cases and test tools, were installed on the test machine by the evaluator according to the instructions in the ECG, Sponsor Test Plan and Evaluator Test Plan. During the evaluation the file system types ext3 and VFAT with the umask of 077 was used for hard disk partitions on the test system. The certification-eal3 rpm and the configuration script contained in the rpm ensured the evaluation compliant system configuration. After running the automated configuration, no further system configuration was performed and only the tools required for testing were installed. The test systems were therefore configured according to the ST and the instructions in the ECG. The evaluator used all the automated test cases provided by the sponsor and ran them on the test systems via the automated driver scripts according to the test plan Test Plan provided by the sponsor. The log files generated by the test cases were analyzed for completeness and failures.

The sponsor provided the following automated test cases:

- The test cases from the LTP, which generate a log file that lists FAIL/PASS for all the test cases contained in this group.
- The 'at' group of tests, which generate a log on Standard Out that contains a list of PASSED/FAILED test cases.
- The ACL test cases, which report ok/failed and summarize the number of failed and passed test cases at the end.
- The OpenSSL test cases, which produced test information on Standard Out that included PASS/FAIL lines.
- The audit test cases, which produced various log files that where summarized by a make command in the end, showing only the FAILs.

The results of the manual test cases were checked according to the expected results in the test plan. All the test results conformed to the expected test results from the test plan.

In addition to running the tests that were provided by the sponsor, according to the test plan from the sponsor, the evaluator decided to run some additional test cases on the provided test systems:

- **Password Quality Tests**: Performed to verify that the password quality settings prevent trivial passwords. See [TPE] section 3.1.
- **Verification of the use of MD5 passwords**: Performed to verify that long passwords can be used on the TOE due to the MD5 algorithm used for storing the passwords instead of using the classic crypt function that truncates passwords at eight characters.
- **Verification the SUID programs do not change the real UID:** Performed to verify that SUID programs do not change the real UID, only the effective UID. See [TPE] section 3.3.
- **Testing of object reuse in regular file system objects**: Performed to check for object reuse in regular files by creating a large spares file and trying to find non-zero data in the spares area.
- **Verification of the use of the PAM subsystem for system access**: Performed to be able to test that the PAM subsystem is used as specified for system access.
- **Check for data import / export with DAC enforcement:** Although no claims in the ST are made about data import and export, the evaluator deemed it necessary to check for the correct functioning of the star utility mentioned for this purpose in the Evaluated Configuration Guide. By testing this utility, the evaluator also had a simple ACL enforcement test.

All tests passed successfully

7.3 Penetration Testing

The approach used to derive penetration tests consisted of the evaluator checking common sources for vulnerabilities of the Linux operating system in general and the TOE. For each vulnerability, the evaluator checked for the following:

- If the reported vulnerability would affect the evaluated configuration of the TOE in its intended environment. If yes, he checked.

- If the reported vulnerability has already been fixed in the evaluated configuration of the TOE. For those that have not been fixed (one was identified – the audit race condition), the evaluator analyzed the potential impact and exploitability.

Besides those vulnerabilities reported in common sources, the evaluator checked other evaluation reports for potential vulnerabilities mentioned there. For those vulnerabilities, the evaluator devised a way to check for the existence or absence of such a hypothetic vulnerability taking into account the fact that for the TOE as an Open Source product the evaluator had full access to the source code.

The evaluator decided to generate only a small number of penetration tests, but instead to perform for some of those an analysis far deeper than usually done for this evaluation level. The reasons for this approach are:

The TOE as an Open Source product is checked for obvious vulnerabilities quite extensively by the Open Source community making the development of high-level, simple penetration tests a rather useless task.

The TOE as an Open Source product is delivered with the full source code, thus allowing the evaluator to perform an analysis to a depth usually not possible for products evaluated at this level.

The evaluator has performed his penetration tests on a TOE that was installed as described in the ST following the description given in the ECG. The penetration testing addressed the Audit and TSF Protection security functions.

The result of the penetration testing can be summarized as follows: The evaluator checked for some hypothetical vulnerabilities using penetration testing and vulnerability analysis techniques. As a result the evaluator did not find as part of his penetration testing any obvious vulnerability of the TOE that is exploitable in the intended TOE environment.

8 Evaluated Configuration

The evaluated configurations are defined as follows:

- The CC evaluated package set must be selected at install time in accordance with the description provided in the Evaluated Configuration Guide and installed accordingly.
- The operating system supports the use of IPv4 and IPv6, only IPv4 is included within the TOE.
- Both installation from CD and installation from a defined disk partition are supported.
- The default configuration for identification and authentication are the defined password based PAM modules. Support for other authentication options (e.g. smartcard authentication) is not included in the evaluation configuration.

- If the system console is used, it must be connected directly to the system and afforded the same physical protection as the server.

The TOE comprises a single server machine (and optional peripherals) listed in Section 5.1 running the system software listed the package list in section 5.2 (a server running the above listed software is referred to as a "TOE server" below).

9 Results of the Evaluation

The Red Hat Enterprise Linux AS Version 4 Update 4 satisfies all of the EAL3 assurance requirements augmented by ALC_FLR.3. The EAL3 assurance requirements augmented by ALC_FLR.3 include the following:

Table 9-1. EAL3+ Assurance Components

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.3 Authorization controls
	ACM_SCP.1 TOE CM coverage
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life Cycle Support(ALC)	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
Tests (ATE)	ATE_COV.2 Analysis of Coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability Assessment (AVA)	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

The Security Target provides a detailed description of how RHEL version 4 Update 4 meets each of the listed components.

10 Validation Comments/Recommendations

The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, Evaluation Assurance Level 3 augmented by ALC_FLR.3 (EAL3), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.3.

The TOE meets the requirements of the Controlled Access Protection Profile (CAPP). Therefore, full compliance is claimed with the requirements of this Protection Profile; also, additional functional and assurance packages beyond those required by CAPP have been included.

The TOE, in its evaluated configuration, performed as expected and should meet the expectations of the customer.

The Evaluation Configuration Guide provided contains the necessary information for a proper installation of the TOE. The guidance provided in this ECG must be strictly adhered to in order to properly install the TOE in its evaluated configuration.

In addition, it shall be noted that the cryptography used in this product was tested using a cipher compliance test approach, which used the methodology proscribed by the NIST Cryptographic Algorithm Validation Scheme. Those security functions included as FIPS Approved functions were tested by the cryptographic test laboratory and validated by NIST's Cryptographic Algorithm Validation Program. The accredited laboratory used the CAVS tool version 5.1, and the results were validated by NIST's Cryptographic Algorithm Validation Program (CAVP). A similar test methodology to that used by NIST was developed for the non-FIPS Approved RC4 algorithm using the ARCFOUR definition as a reference implementation, in order to test for successful implementation of the algorithm. The method is described in the laboratory's "Developed Methods". The implementation of this algorithm (RC4) was NOT validated by NIST nor any other independent party.

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices. The TOE is compliant with the CAPP. The Validator agrees that the CCTL presented appropriate rationales to support the Results of the Evaluation presented in Section 5 of the ETR. Therefore, the Validator concludes that the evaluation and the Pass results for the TOE identified below are complete and correct:

- Red Hat Enterprise Linux AS Version 4 Update 4

11 Security Target

Red Hat Enterprise Linux AS Version 4 Update 4, Security Target for CAPP Compliance, Version 2.8, dated 22 August 2006.

12 Acronyms

ACL	Access Control List
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
API	Application Programming Interface
ATE	Tests
AVA	Vulnerability assessment
CAPP	Controlled Access Protection Profile
CC	Common Criteria [for IT Security Evaluation]
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
CCTL	Common Criteria Testing Laboratory
DAC	Discretionary Access Control
DOD	Department of Defense
EAL	Evaluation Assurance Level
ECG	Evaluation Configuration Guide
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
HLD	High-level Design
I&A	Identification & Authentication
IP	Internet Protocol
IPC	Interprocess Communication
IT	Information Technology
LTP	Linux Test Project
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PAM	Pluggable Authentication Module
PC	Personal Computer
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SF	Security Function
SFP	Security Function Policy

SGI	Silicon Graphics, Inc.
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TP	Test Plan
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
US	United States

13 Bibliography

The following documents were used in compiling this Validation Report:

- Common Criteria EAL3+ Evaluated Configuration Guide for Red Hat
- Enterprise Linux on SGI Hardware
- Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, Part 1 to 3
- Common Criteria EAL3+ Evaluated Configuration Guide for Red Hat Enterprise Linux on SGI Hardware
- Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005
- Red Hat Enterprise Linux AS Version 4 Update 4 Security Target for CAPP Compliance Version 2.8, 22 August 2006
- Evaluator Test Plan for RHEL4 U4, Version 1.0, 11 August 2006
- Red Hat Enterprise Linux AS Version 4 Update 4, Final ETR Version 1.0, 15 September 2006