National Information Assurance Partnership

™

Common Criteria Evaluation and Validation Scheme Validation Report

Unisys Corporation, Unisys Way, Blue Bell, PA 19424

Red Hat Enterprise Linux (RHEL) Advanced Server (AS), Version 3 Update 5 Running on ES7000 Hardware

ACKNOWLEDGEMENTS

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in January 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 3 augmented with ALC_FLR.2.

RHEL AS is a commercial operating system product developed by Red Hat, Inc. It is a version of Linux that has been developed not only to serve as an fully capable operating system, but also to provide a good level of security for commercial environments.

The Unisys ES7000 hardware platforms (specifically, the Unisys ES7000-4xx-M2 series) are mainframes designed and developed by Unisys Corporation. Each of these machines is designed to support numerous 32- or 64-bit Intel microprocessors, respectively, as well as other supporting and peripheral devices (memory, disks, CD and floppy disk drives, network cards, and other I/O devices such as keyboard and mice).

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 3 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC, the Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware Security Target (henceforth referred to as RHEL3), and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.

- The Security Target (ST), describing the security features, claims, and assurances of the product.

- The conformance result of the evaluation.

- The Protection Profile to which the product is conformant.

- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware models 405, 410, 420, 430, and 440
Protection Profile	Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999
Security Target	Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware Security Target, Version 1.0, 4 January 2007
Evaluation Technical Report	Evaluation Technical Report for Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware: • Part 1 (Non-Proprietary), Version 1.0, January, 2007

Item	Identifier
	• Part 2 (Proprietary), Version 1.0, January, 2007
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2
	Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Unisys Corporation
Developer	Unisys Corporation and Red Hat Enterprise
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Mario Tinto, Jason Andryuk, Aerospace Corporation, Columbia, MD

3   Security Policy

In general, the security policies enforced by the TOE are based on the following overarching security objectives:

- **Accountability**. The users of the system shall be held accountable for their actions within the system.

- **Authorization**. Only those users who have been authorized to access the information within the system may access the system.

- **Need to Know**. Only those authorized users that have a 'need to know' for information will be provided access to the protected resources.

More specifically, the security policies implemented by RHEL3 include access control, identification and authentication of user identity, individual accountability for user actions, as well as the protection of the mechanisms that implement the security policies.

3.1   Access Control

Red Hat Enterprise Linux implements Discretionary Access Control (DAC) through the use of standard UNIX permission bits and the POSIX standard Access Control Lists (ACLs). A Discretionary Access Control policy requires mechanisms whereby the access of users (i.e., subjects) to system resources and data (i.e., objects) can be controlled on the basis of user identity, role, and explicit permissions. Mechanisms that implement a DAC policy provide the capability for users to specify the how their personal data objects are to be shared.

Permission bits are associated with objects and specify the permissions (typically, READ, WRITE, EXECUTE) for a specific user, the user's group, and all others (i.e., "world"). Access Control Lists provide the same functionality relative to granting specific permissions, but are considerably more flexible in that they can identify a number of group affiliations for a single user.

The standard UNIX DAC mechanism is permission bits, as is the case with RHEL. However, RHEL implements ACLs as an extended permission mechanism, available at the discretion of the file owner; ACLs are supported only for file system objects.[1]

3.2   Identification and Authentication

RHEL3 provides identification and authentication using user passwords. The quality of the passwords used can be enforced through configuration options controlled by Red Hat Enterprise Linux. Other authentication methods (e. g. Kerberos authentication, token-based authentication) that are supported by RHEL3 as pluggable authentication modules are not part of the evaluated configuration. Functions to ensure medium password strength, limit the use of the su command, and restrict root login to specific terminals are also included.

3.3   Security Audit

RHEL3 provides an audit capability to generate audit records for security relevant events. The administrative user can select which events will be audited and for which users auditing is active.

RHEL3 provides tools for the administrative user that allow extracting specific types of audit events, audit events for specific users and groups, and successful or failed events from the overall audit records collected by RHEL3. Those tools allow an administrative user to save or print the selected audit records in human readable form.

The audit function informs the system administrator via a *syslog* message when the capacity of the audit trail exceeds a configurable limit. The audit function also ensures that no audit records get lost due to exhaustion of the internal audit buffers. Processes that try to create an audit record while the internal audit buffers are full will be blocked until the required resources are available again.

3.4   Security Management

The management of the security-critical parameters of RHEL3 is performed by administrative users. A set of commands that require root privileges are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of RHEL3 against unauthorized access by non-administrative users.

3.5   Protection of the TOE Security Functions

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

---

[1] See Section 6.1.2 of the ST for a fuller discussion of the DAC mechanisms and the algorithm by which access determinations are made.

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.

RHEL3 and the hardware and firmware components are assumed to be physically protected from unauthorized access. The system kernel mediates all access to the hardware mechanisms themselves, other than program visible CPU instruction functions.

RHEL3 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.

3.6 Object Reuse

Although the TOE supports several different types of objects, each is managed by the system such that no pre-existing content is provided to users to whom objects are allocated. That is, whenever an object (e.g., buffers, memory extents, disk space) is allocated to a user process, it is managed such that any data that had previously been in the object (i.e., from an earlier process) is unavailable to the new process.

In short, memory pages are initialized to all zeroes when allocated to a process, IPC objects are also initialized to all zeroes, and file system objects are created with no content (with the exception of directories and symbolic links).

4 Assumptions

The assumptions underlying the evaluation of RHEL3 are all based upon those present in the Controlled Access Protection Profile

4.1 Usage Assumptions

Authorized users are assumed to 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.

It is assumed that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. These administrators are assumed not to be careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrative documentation.

4.2 Environmental Assumptions

The processing resources of the TOE are assumed to be located within controlled access facilities that will prevent unauthorized physical access. All connections to peripheral devices are assumed reside within those boundaries. CAPP-conformant TOEs only address security concerns related to the manipulation of the TOE through its authorized access

points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

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. CAPP-conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address the need to trust external systems or the communications links to such systems. There is also no assumption that networks into which the TOE is connected consist of homogeneous systems, although there is an assumption that they have common management and common policies.

Lastly, it is assumed that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 Clarification of Scope

The TOE includes the hardware platform and all the code that enforces the policies identified (see Section 3). TOE also includes secure communications functions; i.e., SSH V2 and SSL V3).

The administrator tools are not considered to be part of the TSF. The administrator uses the commands that are provided by RHEL for system management; these are utilities that execute in untrusted user space, and are protected by the normal O/S mechanisms that prevent user processes from interfering with each other. Note that system management tools do not enforce TOE security policies, and that the TSF checks that the caller is authorized to invoke the requisite system calls and has the access rights to the objects being accessed.

Also, as noted earlier, the product supports a number of alternate authentication methods (e. g. Kerberos authentication, token-based authentication) as pluggable authentication modules that are not part of the evaluated configuration.

5 Architectural Information

The following architectural description is based on the description presented in Part I of the RHEL3 ETR and in the Security Target.

RHEL3 consists of the following distinct modules:
- File & I/O subsystem – The file and I/O subsystem is a management system for defining objects on secondary storage devices.
- Process Control subsystem – The process management subsystem creates, manipulates, and terminates processes.
- IPC subsystem – The IPC subsystem allow processes to exchange arbitrary amounts of data and synchronize execution. The IPC mechanisms include unnamed pipes, named pipes (FIFOs), the System V IPC mechanisms (consisting of message queues, semaphores and shared memory regions), signals, and sockets.

- Network subsystem – The network subsystem allows Linux systems to connect to other systems over a network. It provides a general purpose framework in which network services are implemented.
- Memory Management subsystem – The memory manager subsystem is responsible for controlling process access to the hardware memory resources.
- Audit subsystem – The audit subsystem records security relevant events in the form of an audit trail and provides tools to an administrative user to configure the subsystem and evaluate audit records.
- Kernel modules subsystem – Kernel modules subsystem supports dynamically loadable kernel modules (object code that can be linked to and unlinked from the kernel at runtime) that are loaded automatically on demand.
- Device drivers subsystem – The device driver subsystem provides a layer of abstraction to other kernel subsystems so they can interact with hardware devices without being cognizant of their internal workings.
- System initialization subsystem – The system initialization subsystem has the sole responsibility of loading the Linux kernel with its required files or (in some cases) other operating systems into memory.
- Identification and Authentication subsystem – The identification and authentication subsystem provides an authentication infrastructure called the Pluggable Authentication Module (PAM) which allows different trusted programs to follow a consistent authentication policy.
- Network applications subsystem – The network applications subsystem includes for example trusted processes and trusted programs that recognize different hosts in the LAN in the IT environment with their IP addresses or with their names.
- System Management subsystem – This subsystem contains the trusted programs used for system management activities.
- Batch Processing subsystem – The batch processing subsystem allows users and system administrators to automate routine maintenance tasks.
- User Level Audit subsystem – This subsystem contains the portion of the audit system that lies outside the kernel.

5.1 File & I/O subsystem

The file and I/O subsystem is a management system for defining objects on secondary storage devices. The file and I/O subsystem interacts with the memory subsystem, the network subsystem, the IPC subsystem, the process subsystem, and the device drivers.

5.2 Process Control subsystem

A process is defined as an instance of a program in execution. Process management consists of creating, manipulating, and terminating a process. Process management is handled by the process management subsystems of the kernel. It interacts with the memory subsystem, the network subsystem, the file and I/O subsystem, and the IPC subsystem.

5.3 IPC subsystem

The Red Hat Enterprise Linux kernel provides a number of inter-process communication mechanisms that allow processes to exchange arbitrary amounts of data and synchronize

execution. The IPC mechanisms include unnamed pipes, named pipes (FIFOs), the System V IPC mechanisms (consisting of message queues, semaphores and shared memory regions), signals, and sockets.

5.4   Network subsystem

The network subsystem allows Linux systems to connect to other systems over a network. It provides a general purpose framework in which network services are implemented. The network subsystem abstracts both of these implementation details so that user processes and other kernel subsystems can access the network without knowing the physical devices and the protocol being used.

5.5   Memory Management subsystem

The memory manager subsystem is responsible for controlling the access of processes to the hardware memory resources. This is accomplished through a hardware memory-management system that provides a mapping between process memory references and the physical memory of the machine. The memory manager subsystem maintains this mapping on a per-process basis, so that two processes can access the same virtual memory address and actually use different physical memory locations. In addition, the memory manager subsystem supports swapping; it moves unused memory pages to persistent storage to allow the computer to support more virtual memory than there is physical memory.

5.6   Audit subsystem

The Linux Audit-Subsystem (LAuS) provides an administrative user with the ability to identify attempted and realized violations of the system's security policy. The audit subsystem records security relevant events in the form of an audit trail and provides tools to an administrative user to configure the subsystem and evaluate audit records. For each action, the auditing facility records enough information about those actions to verify the following:
- the user who performed the action;
- the exact date and time it was performed;
- the success or failure of the action;
- the name, type, device, inode, and the filesystem ID of any data object involved.

5.7   Kernel modules subsystem

Kernel modules are pieces of object code that can be linked to and unlinked from the kernel at runtime. Kernel modules usually consist of a set of functions that implement a file system, a device driver, or other functionalities at the kernel's upper layer. Lower-layer functions, such as scheduling and interrupt management, cannot be modularized. Kernel modules can be used to add or replace system calls. The Red Hat Enterprise Linux kernel supports dynamically loadable kernel modules that are loaded automatically on demand.

5.8   Device drivers subsystem

The TOE supports many different I/O devices, such as disk drives, tape drives, and network adapters. Each of these hardware devices can have its own methods of handling data. The device driver subsystem provides a layer of abstraction to other kernel subsystems so they can interact with hardware devices without being cognizant of their internal workings. Each

supported hardware device has a device driver that is loaded into the kernel during system initialization. The device driver subsystem provides access to these supported hardware devices from user space through special device files in the /dev directory. Valid operations on the device-special files are initialized to point to appropriate functions in the device driver for the corresponding hardware device.

5.9   System initialization subsystem

When a computer with Red Hat Enterprise Linux is turned on, in general, the operating system is loaded into memory by a special program called a boot loader. A boot loader usually exists on the primary hard drive of a system (or other media device) and has the sole responsibility of loading the Linux kernel with its required files or (in some cases) other operating systems into memory.
Each of the architectures capable of running Red Hat Enterprise Linux uses a different boot loader.

5.10 Identification and Authentication subsystem

PAM consists of a set of shared library modules, which provide appropriate authentication and audit services to an application. Applications are updated to offload their authentication and audit code to PAM, which allows the system to enforce a consistent identification and authentication policy, as well as generate appropriate audit records. The following trusted programs are enhanced to use PAM:

- login
- passwd
- su
- useradd, usermod, userdel
- groupadd, groupmod, groupdel
- sshd
- vsftpd
- chage
- chfn
- chsh

5.11 Network applications subsystem

The network applications subsystem contains sshd and vsftpd trusted processes, which interact with the PAM modules to perform authentication. The network application subsystem also includes the xinetd superserver and the ping program. These trusted processes and trusted programs recognize different hosts in the LAN with their IP addresses or with their names. Host names are associated with IP addresses using the /etc/hosts file.

5.12 System Management subsystem

This subsystem contains the trusted programs used for system management activities. They include chage, chsh, chfn, useradd, usermod, userdel, groupadd, groupmod, groupdel, gpasswd, date, and amtu.

5.13 Batch Processing subsystem

Batch processing on Red Hat Enterprise Linux system means to submit a job that will be run when the system load permits. Batch processing allows users to perform CPU-intensive tasks while the system load is low; it also allows users and system administrators to automate routine maintenance tasks. While batch processing provides a convenient feature, it also raises a security issue because a privileged process has to perform a task ordered by a normal user.

5.14 User Level Audit subsystem

This subsystem contains the portion of the audit system that lies outside the kernel. This subsystem contains auditd trusted process, which reads audit records from kernel buffer and transfer them to ondisk audit logs, trusted audit management utilities aucat, augrep, aurun, and audbin , audit logs, audit configuration files, and audit libraries.

6 Documentation

6.1 Evaluation Documentation

The following documentation was used as evidence for the evaluation of the RHEL3:[2]

Assurance Class	Document Title
ASE	Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware Security Target, Version 1.0, 4 January 2007
ACM	• Unisys Configuration Management Evidence Questionnaire, v1.0, 2006/04/24. • Evaluation Team ACM/ALC Questionnaire, v1.0, 2006/12/12. • Red Hat Enterprise Linux Version 3 Update 5 Evaluation Assurance Level 3 Configuration Management Plan, v0.2, 2006/12/13. • Red Hat Enterprise Linux Version 4 Evaluation Assurance Level 4 Configuration Management Plan, 2005/02. • Unisys-developed supply chain applications sample records for RHEL operating system software (after receipt) • Subversion (COTS product that supersedes CVS) sample records for Unisys non-operating system software • Red Hat Enterprise Linux Configuration Management Plan, v0.1, 2005/04/10 • SVN sample records for RHEL operating system software (during development)
ADO	• Unisys Delivery Evidence Questionnaire, Version 0.2, 02/13/06 • Navigating – Unisys Support website – EAL3 Downloads.doc • Common Criteria - EAL3 Validation Configuration Guide for Red Hat Enterprise Linux Version 3 Update 5 on Unisys ES7000 4xx (64bit), December 05, 2006, Version 1.6

---

[2] This documentation list is based on the list provided in the Evaluation Technical Report, Part 1, developed by SAIC.

Assurance Class	Document Title
ADV	• Common Criteria – Functional Specifications for RED HAT Enterprise Linux on Unisys ES7000, Version 1.3, 05/03/06 • Common Criteria Linux Audit-Subsystem Design Documentation, Version 0.2, 05/09/06 • Common Criteria - High Level Design for RED HAT Enterprise Linux on Unisys ES7000, Version 1.6, 1/25/06 • Red Hat man pages (http://www.redhat.com/mirrors/LDP/docs.html#man)
AGD	• Common Criteria – EAL3 Validation Configuration Guide for Red hat Enterprise Linux Version 3 Update 5 on Unisys ES7000 4xx (64bit), December 05, 2006, Version 1.6 • Common Criteria EAL3 Configuration Guide for Red Hat Enterprise Linux on Unisys ES7000, v1.0, 2005/10/03 • Red Hat Enterprise Linux 3 Reference Guide, "rhel-rg-en.pdf" • Red Hat man pages (http://www.redhat.com/mirrors/LDP/docs.html#man)
ALC	• Unisys Life Cycle Evidence Questionnaire, v1.0, 2006/04/24 • Evaluation Team ACM/ALC Questionnaire, v1.0, 2006/12/12 • Red Hat Enterprise Linux Life Cycle Document, v0.2, 2006/04/07 • Unisys on-site visit of the Malvern, PA Unisys facility performed as part of testing, which included inspection of physical access controls and procedures, and interview of staff • Photographs of physical security measures at Red Hat facility in Raleigh, NC
ATE	• Common Criteria EAL3 Testcase Mapping Guide for Red Hat Enterprise Linux Version 3 Update 5 on Unisys ES7000, v1.2, 2006/08/01. • Common Criteria EAL3 Validation Depth of Testing Analysis for Red Hat Enterprise LINUX Version 3 Update 5 on Unisys ES7000 4xx (64bit), v1.1, 2006/01/31. • Common Criteria EAL3 Validation Security Function Verification Test Plan for Red Hat Enterprise Linux Version 3 Update 5 on Unisys ES7000 4xx (64bit), v1.2, 2006/07/19. • Automated test code "\Unisys EAL3\RHEL3 Test scripts" • Automated test code mapping document "0 - EAL3 RHEL3-u5 TestCase Rationale.xls"
AVA	• Common Criteria – EAL3 Validation Vulnerability Analysis for RED HAT Enterprise Linux RHEL3 and 4 on Unisys ES7000, version 1.2, 09/25/06 • Common Criteria – EAL3 Validation Configuration Guide for Red hat Enterprise Linux Version 3 Update 5 on Unisys ES7000 4xx (64bit), December 05, 2006, Version 1.6. • Red Hat Enterprise Linux 3 Reference Guide, "rhel-rg-en.pdf" • Red Hat man pages (http://www.redhat.com/mirrors/LDP/docs.html#man)

6.2 User Documentation

The documentation delivered to the user with the product is that listed for AGD, in the above table.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the RHEL Version 1.1, January 5, 2007.

7.1 Developer Testing

At EAL3, testing must demonstrate correspondence between the tests and the functional specification as well as between the functional specification and the high level design. The vendor testing included both automated and manual tests, and was judged to be extensive and cover all of the security functions identified in the ST as well as each of the defined interfaces. These security functions include:
- Identification and Authentication
- User Data Protection
- Security Audit
- Security Management
- Protection of the TSF

The vendor provided a number of mappings for the test cases:

- Security functions are mapped to SFRs;
- SFRs are mapped to vendor-defined labels/capabilities;
- Vendor-defined labels/capabilities are mapped to subsystems;
- Subsystems are mapped to interfaces;
- Subsystems are mapped to test suites;
- Interfaces are mapped to test case code.

In short, the test case mapping provided by the vendor maps interfaces to test case code, both for the automated and the manual test cases

7.2 Evaluation Team Independent Testing

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran all developer tests and verified the results on one platform, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

7.3 Vulnerability Analysis and Testing

The evaluation team reviewed the developer's strength of function analysis, vulnerability analysis, and misuse analysis. The evaluation team also performed misuse analysis and penetration analysis.

The evaluation team's vulnerability analysis revealed a number of vulnerabilities that were deemed to be potentially applicable. However, further analysis and selected penetration testing led to the conclusion that all issues were either:

- Already included in the developer's analysis;
- Addressed in a prior release;

- Not applicable to the evaluated configuration.

In summary, it was determined that the TOE does not contain exploitable flaws or weaknesses within the parameters of the analysis and testing performed for an EAL3 evaluation.

8   Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware models 405, 410, 420, 430, and 440. To use the product in the evaluated configuration, the product must be configured as specified in the vendor's manual: *Common Criteria – EAL3 Validation Configuration Guide for Red hat Enterprise Linux Version 3 Update 5 on Unisys ES7000 4xx (64bit),* December 05, 2006, Version 1.6.

9   Results of the Evaluation[3]

The evaluation team determined the product to be **CC Part 2 extended, CC Part 3 conformant, CAPP conformant,** and to meet the requirements of **EAL 3 augmented by ALC_FLR.2**. In short, the product satisfies the security technical requirements specified in *Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware Security Target,* Version 1.0, 4 January 2007.

This conclusion was reached as a result of the evaluation team's assessment of the evaluation evidence, along with the execution of the vendor test suite, independent tests, and penetration analysis and testing.

10 Validator Comments/Recommendations

There are no validator comments.

11 Security Target

The Security Target is identified as *Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware Security Target, Version 1.0, 4 January 2007*.

---

[3] The results of the assurance requirements are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL3 augmented with ALC_FLR.2 work units received a passing verdict.

12 Glossary

The following definitions are used throughout this document:

- **Attribute.** A characteristic or trait of an entity that describes the entity; for example, the telephone number of an employee is one of that employee's attributes. An attribute may have a type, which indicates the range of information given by the attribute, and a value, which is within that range.

- **Audit Trail.** Data, in the form of a logical path that links a sequence of events, used for tracing the transactions that affected the contents of a record.

- **Authentication.** Verification of the identity of a user or the user's eligibility to access an object.

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.2, January 2004.

[2] *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.2, January 2004.

[3] *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.2, January 2004.

[4] *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for Red Hat Enterprise Linux (RHEL), Version 3 Update 5 Running on ES7000 Hardware, Part 1 (Non-Proprietary)*, Version 1.0, January 5, 2007.

[8] Science Applications International Corporation. *Evaluation Technical Report for Red Hat Enterprise Linux (RHEL), Version 3 Update 5 and Version 4 Running on ES7000 Hardware Part 2 (Proprietary)*, Version 1.0, January 5, 2007.

[9] Science Applications International Corporation. *Evaluation Team Test Report for Red Hat Enterprise Linux (RHEL), Version 3 Update 5 and Version 4 Running on ES7000 Hardware, ETR Part 2 Supplement (SAIC and unisys Proprietary)*, Version 1.1, January 5, 2007.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Science Applications International Corporation. *Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 4 Running on Unisys ES7000 Hardware Security Target, Version 1.0, 4 January 2007*