Certification Report

EAL 2 Evaluation of Platform Computing Corporation

Platform LSF® HPC 6.2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-49
Version: 1.0
Date: 4 April 2006
Pagination: i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.2*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.2*. This certification report and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS IT Security Laboratory located in Ottawa, Ontario, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 4 April 2006, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html

This certification report makes reference to *LSF*, which is a registered trademark of Platform Computing Corporation.

TABLE OF CONTENTS

Executive Summary

The Platform LSF® HPC 6.2, from Platform Computing Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The Platform LSF® HPC 6.2 manages batch compute jobs on clusters of computer systems. Users use the LSF® to submit jobs that require significant CPU time, memory, and/or disk space. Several server processes running on each system co-ordinate to distribute the load across the cluster. User jobs are submitted using the LSF® HPC 6.2 queuing software and the LSF® HPC determines where jobs will be run.

The LSF® HPC can:

- Utilize computing resources at maximum capacity;
- Take full advantage of high performance network interconnects available on clustered systems and supercomputers;
- Use topology-based scheduling that enables maximum application performance for industry leading interconnects;
- Provide scalability and performance; and
- Utilize an extensive library of third party application integrations.

DOMUS IT Security Laboratory is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 13 March 2006, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the Platform LSF® HPC 6.2, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Platform LSF® HPC 6.2 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report (ETR)[1] for this product indicate that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, version 2.2* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.2*.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The Communications Security Establishment, as the CCS Certification Body, declares that the Platform LSF® HPC 6.2 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation is the Platform LSF® HPC 6.2, from Platform Computing Corporation.

2 TOE Description

The Platform LSF® HPC 6.2 manages batch compute jobs on clusters of computer systems. The primary security features offered by the TOE are as follows:

- Access Control

  Role based access control is enforced for the Cluster Administrator, Queue Administrator and Queue user roles. An access request is granted or denied based on a set of configuration files that define user-to-role and role-to-authorization mappings.

- Audit

  The TOE provides an audit capability that generates audit records for security critical events.

- Security Management

  The TOE provides roles to manage security functions. Only authorized roles are permitted to manage the TOE and perform administrative functions.

- Resource Allocation

  The TOE provides the functionality to allocate resource limitations to ensure that a user or process cannot monopolize a resource and cause a denial of service.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Platform LSF® HPC 6.2 is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: Platform LSF® High HPC 6.2 Security Target EAL 2

Revision: .09
Date: February 21, 2006

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.2*, incorporating all final CC interpretations issued prior to 14 December 2005. The Platform LSF® HPC 6.2 is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;
b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c) Common Criteria EAL 2 conformant, with all the security assurance requirements in the EAL 2 package.

6 Security Policy

The Platform LSF® HPC 6.2 implements the following security policies: role based access control, audit, and resource allocation. Policy detail can be found in Section 5.1, 5.2, 5.4, and Section 6.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Platform LSF® HPC 6.2 should consider the following assumptions regarding usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the Platform LSF® HPC 6.2.

7.1 Secure Usage Assumptions

The system administrators are trusted and neither careless, willfully negligent nor hostile, and will follow and abide by the instructions provided by the administrator/user documentation. Furthermore, the administrators of the TOE have been adequately trained in order for them to securely configure the TOE.

7.2 Environmental Assumptions

The TOE resides in a controlled and physically secure environment.

For more information about the TOE security environment, refer to Section *3* of the ST.

7.3 Clarification of Scope

The Platform LSF® HPC 6.2 provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

The Platform LSF® HPC 6.2 provides a multiprocessing computing environment that permits software applications (jobs) to run concurrently on several different hosts (processors), thus reducing the execution time. The Platform LSF® HPC 6.2 is comprised of one or more clusters, each of which includes the following:

- Submission Hosts which are responsible for submitting jobs that require processing.
- A Master Host which controls the allocation of these jobs to the hosts that will perform the processing. The Master Host acts as a coordinator for the Cluster, performing all the scheduling and dispatching tasks.
- Compute Hosts, also called Execution Hosts, which are responsible for executing the jobs that have been assigned to them.
- A Master Candidate Host which is a Compute or Submission Host that can assume the role of Master Host in the event of a failure on that system.

All hosts take on the designations of Client or Server. A Client, as typified by a Submission Host, is only capable of submitting jobs to the Master Host. It cannot assume any other role. A Server is capable of submitting jobs, like a Client, but it is also capable of performing the Master Host and/or Compute Host functions. In the event that the Master Host goes down, one of the Server Hosts called a Master Candidate Host will assume its role.

Before being processed by the Master Host, all batch jobs are placed into a queue. Queues are system-wide, i.e., they are not associated with a specific host. It is the job of the Master Host to determine which Compute Host is to receive the job. Each queue is defined by a unique set of job control and execution parameters. It is also possible to submit interactive jobs to a queue. In this case, I/O is directed to a session running on a specific terminal where the job originated. The interactive session must be completed before the next job can be submitted to that session.

For additional architectural information please refer to Chapter 2 of the ST.

9 Evaluated Configuration

The TOE requires support from the underlying operating system for some security functionality. For the purpose of this evaluation, the operating system is Red Hat Enterprise Linux AS version 3 Update 3. This version of Linux has been CC certified at the EAL 3+ level.

The TOE includes the Multi-Cluster option which allows organizations to have separate, independently managed clusters. Communication between the clusters is secured by VPN appliances. For evaluation purposes, two clusters were created, and two Sonic Wall TZ 170 devices were deployed to protect the communication channel between them.

10 Documentation

The documentation for Platform LSF® HPC 6.2 consists of:

- Installation and Setup for Platform LSF HPC 6.2: Common Criteria Evaluated Configuration;
- Administering Platform LSF 6.2;
- Using Platform LSF HPC 6.2;
- Using Platform LSF Multi-Cluster;
- Platform LSF Reference Version 6.2; and
- Running Jobs on Platform LSF 6.2.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Platform LSF® HPC 6.2, including the following areas:

Configuration management: An analysis of the Platform LSF® HPC 6.2 development environment and associated documentation was performed. The evaluators found that the Platform LSF® HPC 6.2 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the Platform LSF® HPC 6.2 during distribution to the consumer. The evaluators examined and

tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Platform LSF® HPC 6.2 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Platform LSF® HPC 6.2 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The Platform LSF® HPC 6.2 Security Target has no claims for strength of function. The evaluators examined the developer's vulnerability analysis, and found that it sufficiently described each of the potential vulnerabilities along with sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases and all evaluation deliverables to provide assurance that the developer had considered all potential vulnerabilities. Limited penetration testing and source code review were conducted by evaluators, which demonstrated potential vulnerabilities not exploitable in the intended operating environment of the Platform LSF® HPC 6.2.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the ETR.

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

12.2 Independent Functional Testing

During this evaluation, the evaluators developed and conducted independent functional tests by examining the design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results.

The tests focused on:

1. audit;
2. role based access control;
3. security management; and
4. resource allocation.

Tests were selected which demonstrate that the TOE satisfies the security functional requirements specified in the Security Target.

12.3 Independent Penetration Testing

During this evaluation, the evaluator developed limited independent penetration tests following the examination of the developer's vulnerability analysis and test activities, as well as the review of functional specification, high-level design, guidance documentation, and installation guidance. Furthermore, the evaluator inspected a key subset of the source code where the TOE interacts with the IT environment in order to supplement the penetration testing. The examination of source code focuses on the various servers' enforcement of role based access control when a job is submitted, and establishment of the running environment for the job submitted by the user. Penetration testing and source code review did not uncover any exploitable vulnerabilities nor did it reveal any potentially harmful system interaction for the Platform LSF® HPC 6.2 in the intended operating environment.

12.4 Conduct of Testing

The Platform LSF® HPC 6.2 was subjected to a comprehensive suite of formally-documented, independent functional tests and limited penetration tests. The testing took place at the DOMUS IT Security Laboratory located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent tests and penetration tests.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and independent functional tests yielded the expected results, giving assurance that the Platform LSF® HPC 6.2 behaves as specified in its ST and functional specification. The penetration testing resulted in a PASS verdict, as the evaluator was unable to exploit any of the identified potential vulnerabilities in the Platform LSF® HPC 6.2 in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2** level of assurance. The overall verdict for the evaluation is a **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The TOE requires support from the underlying operating system for some security functionality, such as identification and authentication. It is assumed to run in a non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

The TOE includes the Multi-Cluster option which allows organizations to have separate, independently managed clusters. VPN appliances should be deployed to protect communications across the cluster boundary.

For more information about the security requirements on the IT environment, refer to Section *3* of the ST. The Platform LSF® HPC 6.2 also includes comprehensive guides for the installation, configuration, administration and operation of the product.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Arrangement on the Recognition of Common Criteria Certificates

CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HPC	High Performance Computing
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LSF	Load Sharing Facility
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 311, September 2004.

b) Common Methodology for Information Technology Security Evaluation, Evaluation and Methodology, Version 2.2, Revision 311, September 2004.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Evaluation Technical Report (ETR) Platform LSF HPC 6.2, Version 1.0, 14 April 2006.

e) Platform LSF HPC 6.2 Security Target EAL 2, Revision 0.09, 21 February 2006.