National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

For

VMware ESX Server 2.5.0 and VirtualCenter 1.2.0

Report Number: CCEVS-VR-06-0013

Dated: March 27, 2006

Version: 1.7

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

ACKNOWLEDGEMENTS

Validator

Nicole Carlson
Stuart Schaeffer, Senior Validator
The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Michelle Ruppel
Josh McCally
Mark Plascencia
Steve Wilson
InfoGard Laboratories
San Luis Obispo, California

Table of Contents

1 EXECUTIVE SUMMARY

This report documents assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the two VMware components, ESX Server 2.5.0 and VirtualCenter 1.2.0, that comprise the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the InfoGard Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, California, United States of America, and was completed in February 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, produced by InfoGard. The evaluation determined that the product is both Common Criteria Part 2 extended and Part 3 Conformant, and meets the assurance requirements of EAL 2. The product does not claim conformance with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE comprises two components within the larger VMware product: ESX Server 2.5.0 and VirtualCenter 1.2.0. The VMware product provides a middleware layer that effectively virtualizes physical computing resources (e.g. CPUs of a particular architecture) into a pool of logical computing resources. Virtual machines may then be run on the logical computing resources as if they were being run on physical resources. VirtualCenter 1.2.0 allows the centralized management and deployment of virtual machines; ESX Server 2.5.0 acts as a virtualization layer on x86 Server architecture hardware and mediates access to physical resources of the machine.

During this evaluation, the validators monitored the activities of the InfoGard evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., work units of the Common Evaluation Methodology (CEM)), and reviewed successive versions of the Evaluation Technical Report (ETR) and test reports. The validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validator concludes that the InfoGard findings are accurate, the conclusions justified, and the conformance claims correct.

2 IDENTIFICATION

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

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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	VMware ESX Server 2.5.0 and VirtualCenter 1.2.0
Protection Profile	None
Security Target	*VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Security Target*, Version 1.6.7, dated March 10 2006
Evaluation Technical Report	*Evaluation Technical Report for VMware ESX Server 2.5.0 and VirtualCenter 1.2.0*, version 1.1, March 10 2006
Conformance Result	Part 2 extended and Part 3 Conformant, EAL 2
Sponsor	VMware
Developer	VMware
Evaluators	InfoGard Laboratories
Validator	The Aerospace Corporation

3 SECURITY POLICY

No organizational security policies apply.

4 ASSUMPTIONS [1]

4.1 Usage Assumptions

A.DBMS The VirtualCenter and the VirtualCenter Database are installed on the same physical server.

A.GENPUR There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE except within a Virtual Machine on the ESX Server. Furthermore, the VirtualCenter Database is not used for any purpose except that of the VirtualCenter.

A.NOEVIL Administrators of the TOE are non-hostile, appropriately trained, and follow all user and administrator guidance.

4.2 Environmental Assumptions

It is assumed that the IT environment provides support commensurate with the expectations of the TOE. This is achieved by using evaluated products (or products in evaluation at the time of the writing of this VR) in the environment. The expectations of the TOE with respect to the security provided by the IT environment are captured in the ST in the environmental objectives, but *were not* verified by the evaluation.

A.PHYSICAL The TOE is located within a physical area that protects the TOE from unauthorized physical access.

A.SANS When the TOE uses a Storage Area Network, it is on a private, physically protected network and is protected from unauthorized physical access.

[1] Information drawn from *VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Security Target v1.6.7*, dated March 10 2006

5 ARCHITECTURAL INFORMATION[2]

Modern computers ("physical devices") consist of a set of hardware (e.g. a CPU of a certain architecture, memory of a certain size and configuration) that runs an operating system (e.g. Microsoft Windows, Linux). An operating system runs programs; a program may be designed to emulate a computer ("virtual device").

The TOE consists of two components, VMware ESX Server 2.5.0 and VirtualCenter 1.2.0, that operate within the framework of a larger product, VMware. VMware allows users to create virtual machines within a single physical machine, each virtual machine running a separate copy of an operating system (the "guest" operating systems) while the underlying machine runs its own its virtualization layer. Multiple virtual machines may be run on the same physical device. In effect, the physical resources offered by a number of physical machines (e.g. processing power, memory resources) are abstracted into a pool of virtual resources, which may then be drawn on by some number of virtual machines.

The TOE components facilitate use and management of multiple virtual machines located on multiple physical devices. ESX Server 2.5.0 provides a virtualization layer between the physical hardware and the guest operating systems. VirtualCenter 1.2.0 allows the management (including deployment and maintenance) of multiple virtual machines, all from a single central location.

6 DOCUMENTATION

The following documentation was used as evidence for the evaluation of VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Authentication Server and Key Server components:[3]

6.1 Design documentation

Document	Version	Date
VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Design Documentation and Correspondence	1.0.7	February 23, 2006

[2] Drawn from *VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Security Target*; version 1.6.7, March 10 2006

[3] This documentation list is extracted from the *VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Final Evaluation Technical Report*, version 1.1 (March 10 2006)

6.2 Guidance documentation

Document	Version	Date
VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Administrator Guidance Supplement	1.0.7	February 23, 2006
VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Installation Guidance Supplement	1.9.3	February 23, 2006
VMware ESX Server 2.5 Administration Guide	20041129	November 29, 2004
VMware ESX Server 2.5 Installation Guide	20041206	December 6, 2004
VMware VirtualCenter User's Manual	1.2	December 2, 2004
VMware ESX Server Manual Pages, extracted from ESX Server 2.5.0 code		

6.3 Configuration Management documentation

Document	Version	Date
EAL 2 Configuration Management Documentation, VMware ESX Server 2.5.0 and VirtualCenter 1.2.0	1.2.2	February 23, 2006

6.4 Delivery and Operation documentation

Document	Version	Date
ESX Server 2.5.0 and VirtualCenter 1.2.0 Delivery Procedures Document	1.0	February 21, 2006
VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Administrator Guidance Supplement	1.0.7	February 23, 2006
VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Installation Guidance Supplement	1.9.3	February 23, 2006

6.5 Test documentation

Document	Version	Date

VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Test Documentation Supplement	1.0.5	February 23, 2006
VMware ESX Server 2.5.0 EAL2 Test Design Specification	1.7.8	February 23, 2006
VMware VirtualCenter 1.2.0 EAL2 Test Design Specification	1.6	February 23, 2006

6.6 Vulnerability Assessment documentation

Document	Version	Date
VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Common Criteria Vulnerability Analysis	0.9	February 15, 2006

6.7 Security Target

VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Security Target	1.6.7	March 10, 2006

7 IT PRODUCT TESTING

7.1 Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL 2.

The developer's tests consisted of a suite of tests that covered the security functions claimed in the ST. The evaluation team chose to run approximately 75% of these tests. The tests verified the basic functionality of the TOE, and exercised the parameters and verified the exception conditions documented in the user and administrative guidance.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for, the function being tested. The evaluators also verified that the test documentation showed results that were consistent with the expected results for each test case.

7.2 Evaluator Testing

7.2.1 Functional Testing

In addition to developer testing, the CCTL conducted its own suite of functional tests, which were created independently of the developer. These also completed successfully. Among them were tests designed to test whether:

- Logins, whether successful or unsuccessful, generated audit records;
- Reliable audit logs were created and kept;
- Memory was never shared across virtual machines; and
- Unauthenticated access to TOE-mediated functionality was not possible.

7.2.2 Vulnerability Testing

The evaluators developed vulnerability tests to address both management functions and security functions controlling access to the TOE, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE, such as:

- Accessing privileged functions, data, or websites was only possible for VirtualCenter Administrators;
- Data en route to and from the TOE was not human-readable;
- Disconnection in service triggered a mandatory re-authentication for TOE users.

7.2.3 Penetration testing

The evaluation team attempted to break the security of the TOE with the following results:

- Deliberately inputting information that the product is not designed to accept (e.g. unusually long or strangely formatted input). The TOE rejected the faulty input and continued to run correctly.
- Altering critical system data, such as a critical file that is not expected to be human-readable. The TOE detected the change and exited.
- Attempts to escalate privileges by changing a URL for a web page internal to the TOE to point to a privileged internal URL. The TOE denied access.

8 EVALUATED CONFIGURATION

Both components of the TOE run within the context of a larger product, VMware. The TOE runs on a number of different x86 architecture server platforms. Hence, hardware on which the TOE runs is outside the scope of the TOE and was not part of the evaluation. The hardware configuration used for the purpose of the evaluation is provided here for reference.

- Pentium 4 2.8GHz (VirtualCenter Server)
  - 512 Mb RAM
  - 10/100Mbps NIC
  - Windows XP Professional SP2
- Pentium 3 927MHz (VirtualCenter Client)
  - 256Mb RAM
  - 10/100Mbps NIC
  - Windows XP Professional SP2
- Dual Pentium 4 Xeon 3.2 GHz (ESX Server)
  - 2 GB RAM
  - Dual 10/100/1000Mbps NICs
- 2 NetGear GS105 fast Ethernet Gigabit Switches
- 2 Fibre Channel Host Bus Adapters (HBAs)
- Fibre Channel SAN
- Fibre Channel Switch

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.2, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 2.2, dated August 1999 [6]; and all applicable International Interpretations in effect on 1 April 2004. The evaluation confirmed that the VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 product is compliant with the Common Criteria Version 2.2, functional requirements (Part 2), and assurance requirements (Part 3) for EAL2. The details of the evaluation are recorded in the CCTL's evaluation technical report, *Evaluation Technical Report for the VMware ESX Server 2.5.0 and VirtualCenter 1.2.0*. The product was evaluated and tested against the claims presented in the *VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Security Target v 1.6.7*, dated March 10 2006.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme Publication Number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The Security Target evaluation ensures that the ST contains a description of the environment in which the TOE is expected to run, as well as an accounting of security requirements claimed to be met by the TOE.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each ACM CEM work unit. The ACM evaluation ensures that the TOE may be uniquely identified. The evaluation team found that the developer uses version control software to accept, control, and track changes to the TOE's source code as well as to TOE-related documents. Bug fixes and updates can be uniquely identified: the version number is a three-part number *x.y.z* where *x* is the major release number, *y* is the minor release number, and *z* is a maintenance release number. The unique TOE identifier is, therefore, a pair of product name/version numbers, (ESX Server 2.5.0, VirtualCenter 1.2.0). A unique build number is associated with each three-digit version number.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each ADO CEM work unit. The purpose of the ADO evaluation is to make sure that the procedures in place to deliver, install, and configure the TOE securely are adequate. The TOE is only available from the developer's website, where the results of a one-way hash (MD5) are also published. Its integrity is assured at the delivery site by performing the same function and comparing the results. The team also tested the installation and configuration procedures in the Installation Guide to ensure that the prescribed procedures result in a secure installation.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it an acceptably complete explanation of how the TSF provides its security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also verified that the actual implementation of the TOE was a correct and complete interpretation of the high-level design.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team verified that the user guidance was sufficient to describe how to use the operational TOE, and that the administrator guidance was sufficient to describe how to securely administer the TOE. The team found that the guidance documents were, in fact, adequate guidance for these purposes.

9.6 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ensured that the TOE performs as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team, in addition to executing a sample of the vendor test suite, devised and ran an independent set of functional tests. The team also performed penetration tests, which did not uncover any vulnerabilities. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.7 Vulnerability Assessment Activity (AVA)

The evaluation team applied each AVA CEM work unit. This work unit, in addition to the development and execution of penetration tests, requires two separate analyses:

1. a strength of function (SOF) analysis determines whether the claimed protection level is substantiated;

2. a vulnerability analysis examines public information to determine if there are known vulnerabilities that may affect the TOE (for example, vulnerabilities affecting the underlying operating system).

The developer submitted their own analyses, which the evaluation team examined in addition to their analyses, as well as the results of testing. They found that the (single) SOF claim, a claim of SOF-Basic for password strength, was met; and that the known potential vulnerabilities do not affect the TOE.

9.8 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence verifies that the claims in the ST are met. Additionally, the evaluation team’s performance of a subset of the vendor tests suite, the independent tests, and the penetration testing also demonstrated the accuracy of the claims in the ST.

10 VALIDATOR COMMENTS

The TOE makes use of cryptographic modules in order to fulfill some security functions. Cryptographic modules are evaluated under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2, a separate standard from the Common Criteria; the cryptographic functions were not evaluated further during this evaluation. Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate.

11 SECURITY TARGET

VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Security Target, v 1.6.7, March 10 2006

12 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Security Target, v 1.6.7, March 10 2006

[8] Evaluation Technical Report for VMware ESX Server 2.5.0 and VirtualCenter 1.2.0, version 1.1, March 10, 2006