Certification Report

EAL 2+ Evaluation of

Symantec™ Critical System Protection

Version 5.0.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-52-CR
Version: 1.0
Date: 27 November 2006
Pagination: i to v, 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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, applies 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 (CSE).

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 Electronics Warfare Associates-Canada, Ltd located in Ottawa, Ontario.

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 27 November 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 (CPL) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org.

This certification report makes reference to the following trademarked names:

- Microsoft, Windows, Windows Server, and SQL Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Java is a trademark of Sun Microsystems, Inc, in the United States and other countries.
- Apache Tomcat and Tomcat are trademarks of the Apache Software Foundation.

- Symantec is a trademark of Symantec Corporation in the United States and/or other countries.

TABLE OF CONTENTS

Executive Summary

The Symantec™ Critical System Protection v5.0.5 (SCSP), from Symantec Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation.

The SCSP is a software-only implementation of a host-based intrusion detection and prevention system, designed to protect an enterprise's internal network. The intrusion detection capabilities monitor files, registry keys and system logs to allow suspicious activity to be identified and reported; the intrusion prevention capabilities mediate access to system resources, such as registry keys, operating system files, important application files, and devices thereby preventing attacks from occurring. The SCSP is comprised of SCSP Agents, the SCSP Management Server, and the SCSP Management Console. SCSP Agents are software entities installed on various servers, workstations, and databases that are to be protected, and apply intrusion detection and prevention policies. The user responsible for managing the SCSP system creates intrusion detection and prevention policies using the SCSP Management Console (a Java™ application running on a workstation), sends those policies to the SCSP Management Server, which in turn pushes the policies down to the SCSP Agents. The SCSP Management Server (also implemented in Java™) is the central management server for the SCSP system, and provides functionality for storing, updating and distributing to the SCSP Management Console and the SCSP Agents all enforcement policies, configuration settings, log events, and alerts.

Electronics Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 6 November 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 SCSP, the security requirements, and the level of confidence (evaluation assurance level) to which the product is intended to satisfy the security requirements. Consumers 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 provide sufficient evidence that it meets the EAL 2+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic flaw remediation.

[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.

CSE, as the CCS Certification Body, declares that the SCSP 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 Symantec™ Critical System Protection, v5.0.5, from Symantec Corporation (hereafter referred to as the SCSP).

2 TOE Description

The SCSP is a software-only implementation of a host-based intrusion detection and prevention system, designed to protect an enterprise's internal network. The intrusion detection capabilities monitor files, registry keys and system logs to allow suspicious activity to be identified and reported; the intrusion prevention capabilities mediate access to system resources, such as registry keys, operating system files, important application files, and devices thereby preventing attacks from occurring. The SCSP is comprised of SCSP Agents, the SCSP Management Server, and the SCSP Management Console. SCSP Agents are software entities installed on various servers, workstations, and databases that are to be protected, and apply intrusion detection and prevention policies. The user responsible for managing the SCSP system creates intrusion detection and prevention policies using the SCSP Management Console (a Java™ application running on a workstation), sends those policies to the SCSP Management Server, which in turn pushes the policies down to the SCSP Agents. The SCSP Management Server (also implemented in Java™) is the central management server for the SCSP system, and provides functionality for storing, updating and distributing to the SCSP Management Console and the SCSP Agents all enforcement policies, configuration settings, log events, and alerts.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the SCSP is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: Symantec Corporation Symantec Critical System Protection v5.0.5 Security Target
Version: 1.0
Date: 31 October 2006

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3 August 2005*, for conformance to the *Common Criteria for Information Technology Evaluation, Version 2.3 August 2005.*. The SCSP v5.0.5 is:

a. Common Criteria Part 2 extended, with security functional requirements based upon functional requirements in Part 2 except for three explicitly stated requirements: IDS_SDC.1 – System data collection; IDS_RDR.1 – Restricted data review; and IDS_STG.1 – Guarantee of system data availability.
b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.
c. Common Criteria EAL 2 augmented, containing all security assurance requirements from EAL 2, as well as ALC_FLR.1 - Basic flaw remediation.

6 Security Policy

The SCSP enforces host-based Intrusion Detection and Intrusion Protection (IDP) policies. The Intrusion Detection policies are applied to identify suspicious activities occurring on the hosts; the Intrusion Prevention policies are applied to control access to host resources. SCSP IDP policy detail can be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the SCSP should consider assumptions about 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 SCSP.

7.1 Secure Usage Assumptions

Personnel authorized to install, configure, and operate the SCSP possess appropriate training, are not willfully negligent or hostile, and will adhere to the procedures for secure usage of the product.

7.2 Environmental Assumptions

The SCSP is located within controlled access facilities that provide physical security.

7.3 Clarification of Scope

The SCSP provides a level of protection that is appropriate for a non-hostile and well-managed user community. 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 hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

The SCSP is a software-only implementation of a host-based intrusion detection and prevention system (IDS) comprising SCSP Agents, an SCSP Management Server, and an SCSP Management Console.

SCSP Agent. The SCSP Agent is a software application that is installed on the servers, workstations, and databases that are to be protected. The Agent enforces the SCSP IDS policies that are pushed down from the SCSP Management Server.

SCSP Management Server. The SCSP Management Server is the central management server for the SCSP system. The Server provides the functionality for storing, updating and distributing to the Console and Agents all enforcement policies, configuration settings, log events, and alerts. The Server is also responsible for registering Agents, authenticating the Console and Agents, and managing reporting, operators and roles. The Server stores all data used and collected by the system, such as the policies and logs. Communication with the Server is initiated by the Agents and the Console via Secure Hyper-Text Transfer Protocol (HTTPS).

SCSP Management Console. The SCSP Management Console provides the Graphical User Interface (GUI) through which the operator accesses the Management Server.

9 Evaluated Configuration

The evaluated configuration for the SCSP comprises:

- SCSP Agent v5.0.5 running on Windows® XP Professional Service Pack 2 or Windows® Server 2003;
- SCSP Management Server v5.0.5 and the Microsoft® SQL Server Desktop Engine database running on Windows® Server 2003, Java™ Runtime Environment (JRE), and Apache Tomcat™ Server; and
- SCSP Management Console v5.0.5 running on Windows® XP Professional Service Pack 2 or Windows® Server 2003, Java™ Swing, and Java™ Runtime Environment (JRE).

10 Documentation

The documents provided to the consumer are:

- Symantec Critical System Protection Installation Guide, Documentation Version 5.0.5;

- Symantec Corporation Symantec Critical System Protection v5.0.5 Installation Guide v5.0.5 Supplement , Documentation Version 0.4, 16 October 2006;
- Release Notes Symantec™ Critical System Protection;
- Symantec Critical System Protection Administration Guide, Documentation Version 5.0.5;
- Symantec Corporation Symantec Critical System Protection v5.0.5 Administration Guide v5.0.5 Supplement , Documentation Version 0.4, 7 August 2006;
- Symantec Critical System Protection Prevention Policy Reference Guide, Documentation Version 5.0.5; and
- Symantec Critical System Protection Detection Policy Reference Guide, Documentation Version 5.0.5.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the SCSP, including the following areas:

Configuration management: An analysis of the SCSP development environment and associated documentation was performed. The evaluators found that the SCSP 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.

Secure 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 SCSP 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 SCSP 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 SCSP administrator guidance documentation[2] and determined that it sufficiently and unambiguously described how to

[2] The SCSP has administrators only, and no users, and thus no user guidance documentation

securely administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the documented flaw remediation procedures. The evaluators concluded that procedures are in place to track flaws, identify corrective actions, and distribute the flaw information and corrections.

Vulnerability assessment: The SCSP strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the SCSP and found that it sufficiently described each of the potential vulnerabilities along with a 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 has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessment of 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 [3].

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 evaluator developed independent functional tests by examining 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:

[3] 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

- Audit;
- Data protection;
- Identification and authentication;
- Security roles;
- Intrusion detection and prevention functionality; and
- Protection of the security functions.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, limited independent evaluator penetration testing was conducted. Penetration testing did not uncover any exploitable vulnerabilities for the SCSP in the anticipated operating environment.

12.4 Conduct of Testing

The SCSP was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place both at the Symantec Corporation facility in Columbia, Maryland and at the Information Technology Security Evaluation and Test (ITSET) Facility at Electronics Warfare Associates-Canada, Ltd. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the Evaluation Technical Report (ETR).

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the SCSP behaves as specified in its ST and functional specification.

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 **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The SCSP is straightforward to configure, use and integrate into a network.

15 Glossary

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

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDP	Intrusion Detection and Intrusion Protection
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SCSP	Symantec™ Critical System Protection
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, CCIMB-2005-08-001/002/003, Version 2.3 August 2005.

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2005-08-004, Version 2.3 August 2005.

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

d) Symantec Critical System Protection v5.0.5 Security Target, Version 1.0, 31 October 2006.

e) Evaluation Technical Report (ETR) Symantec Critical System Protection v5.0.5, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-52, Document No. 1526-000-D002, Version 1.1, 3 November 2006.