Certification Report

EAL 3+ Evaluation of Shavlik Security Suite v8.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-131-CR
Version: 1.0
Date: 8 July 2010
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has 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 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 Canada, 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 Communications Security Establishment Canada, 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 Canada.

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/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration 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, 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 8 July 2010, 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) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- Shavlik NetChk Protect, Shavlik NetChk Configure, Shavlik Security Intelligence, Shavlik NetChk Agent, and the Shavlik Technologies logo are either trademarks or registered trademarks of Shavlik Technologies, LLC.

TABLE OF CONTENTS

Executive Summary

The Shavlik Security Suite v8.0, from Shavlik Technologies, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Shavlik Security Suite v8.0 simplifies and automates Information Technology (IT) operations, enabling organizations to reduce their effort on critical functions including system discovery, patch management, and configuration management. The Suite allows organizations to:

- Manage security patches;
- Assess and update system security configurations; and
- Review all system security information from one easy-to-use dashboard.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 16 June 2010 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 Shavlik Security Suite, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in 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 3 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that Shavlik Security Suite v8.0 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the

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

CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Shavlik Security Suite v8.0, from Shavlik Technologies.

2 TOE Description

Shavlik Security Suite v8.0 simplifies and automates the systems management challenges relevant to today's Information Technology (IT) environments, enabling organizations to reduce their effort on critical functions including system discovery, patch management, and configuration management. The Suite allows organizations to:

- Manage security patches;
- Assess and update system security configurations; and
- Review all system security information from one easy-to-use dashboard.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Shavlik Security Suite v8.0 is identified in Section 1.4.2 of the Security Target (ST).

4 Security Target

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

Title: Shavlik Security Suite v8.0 Security Target
Version: 1.0
Date: 16 June 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

Shavlik Security Suite v8.0 is:

a. *Common Criteria Part 2 extended*, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - FDC_ANA.1 (EXP) System Analysis;
    - FDC_SCN.1 (EXP) System Scan;

- FDC_STG.1 (EXP) Scanned Data Storage; and
- FAU_GEN.1 (EXP) Audit data generation.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

Shavlik Security Suite v8.0 implements a role-based access control policy to control user access to administrative functions, as well as an information flow control policy concerned with mediating access to machine-scanning, patch-deployment and configuration-deployment functionality; details of these security policies can be found in Section 6.2.2 of the ST.

In addition, Shavlik Security Suite v8.0 implements policies pertaining to security audit, user data protection, identification and authentication, security management, self protection, resource utilization and data collection. Further details on these security policies may be found in Section 1.4.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Shavlik Security Suite v8.0 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system;
- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and
- The users who manage the TOE are not careless, negligent, or willfully hostile, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE environment provides the network connectivity required to allow the TOE to provide secure patch and configuration management functions;

- The IT environment provides the TOE with the necessary reliable timestamps;
- The TOE is located within a controlled access facility;
- All ports needed for proper operation of the TOE will be opened at the firewall. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate;
- The TOE environment will provide identification and authentication functions for users attempting to manage and use the TOE;
- The environment provides a sufficient level of protection to secure communications between distribution servers (if deployed), agents (if deployed) and other TOE components; and
- A FIPS 140-2 validated cryptographic module in the TOE Environment provides all cryptographic functionality for the TOE.

7.3 Clarification of Scope

The following product functionality is not part of the evaluated configuration of the TOE:

- Shavlik NetChk Protect “ping-back mode”;
- Malware detection and removal; and
- Application control.

8 Architectural Information

The TOE consists of the following three products, which can further be broken down into following high-level architectural components as described below:

Shavlik NetChk® Protect v7.5: Simplifies enterprise-wide vulnerability management, providing agent-less patch scanning, and patch deployment from one console.

- **NetChk Protect Console.** The NetChk Protect Console component provides the main management interface for the NetChk Protect components. The main functionality provided by the NetChk Protect Console is the ability to schedule scans of the machines on the local network for the latest patch configurations, and update the patches for those machines as needed. In order to manage the NetChk Protect Console, administrators use a GUI located on the NetChk Protect Console.
- **NetChk Protect Scheduler.** The NetChk Protect Scheduler is a small piece of code that the NetChk Protect Console can send to be installed on a target machine to

handle patch installations. The NetChk Protect Scheduler loads jobs that are batch files containing patch installation instructions from the NetChk Protect Console. After the patch installation is complete, the NetChk Protect Scheduler can either remain running or dormant on the system, or it can remove itself from the system entirely. The NetChk Protect Scheduler may also remove patch installation files after a patch deployment, if configured to do so.

- **NetChk Protect Agent.** The NetChk Protect Agent provides much of the same functionality as a NetChk Protect Console, but it only provides its functionality to the local machine where it is installed. All functionality available via the NetChk Protect Agent is dependent on the agent policy that is configured when the NetChk Protect Agent is initially deployed. The NetChk Protect Agent provides its own thick-client GUI for the user of the workstation where it is installed, and allows that user to run scans and deploy patches through the NetChk Protect Agent.

Shavlik NetChk® Configure v4.2: An agent-less compliance management solution that simplifies and automates the management of critical system and security configurations. It enables organizations to conform to emerging regulations, meet compliance objectives, and reduce the organization's risk of exposure.

Shavlik Security Intelligence™ v4.2: An intuitive, customizable Web-based dashboard that allows organizations to integrate multiple data sources (including Shavlik NetChk Protect, Shavlik NetChk Configure, and others) at one location, providing one unified and comprehensive view. For this evaluation, no claims have been made against the functionality provided by the Shavlik Security Intelligence component of the TOE.

Further details about the system architecture are proprietary to the developer, and are not provided in this report.

9 Evaluated Configuration

Shavlik Security Suite v8.0 is a patch and configuration management software suite which is installed on general-purpose computing hardware running Microsoft Windows operating systems (OS). The TOE is installed on a network in a distributed manner. The TOE is comprised of the following:

- Shavlik NetChk® Protect v7.5 build 2716;
- Shavlik NetChk® Configure v4.2 build 20; and
- Shavlik Security Intelligence™ v4.2 build 02032010.

The publication entitled Shavlik Security Suite v8.0 Common Criteria Guidance Documentation Supplement describes the procedures necessary to install and operate the TOE in its evaluated configuration.

10 Documentation

The Shavlik Technologies documents provided to the consumer are as follows:

- Shavlik NetChk Protect 7.5 Administration Guide;
- Shavlik NetChk Protect 7.5 Installation & Setup Guide;
- Shavlik NetChk Configure 4.2 Installation Guide;
- Shavlik NetChk Configure 4.2 Administration Guide; and
- Shavlik Security Suite 8.0 Common Criteria Guidance Documentation Supplement.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Shavlik Security Suite v8.0, including the following areas:

Development: The evaluators analyzed the Shavlik Security Suite v8.0 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Shavlik Security Suite v8.0 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Shavlik Security Suite v8.0 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Shavlik Security Suite v8.0 configuration management system and associated documentation was performed. The evaluators found that the Shavlik Security Suite v8.0 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well- developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment

to protect the confidentiality and integrity of the Shavlik Security Suite v8.0 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Shavlik Security Suite v8.0 during distribution to the consumer.

The evaluators reviewed the flaw reporting procedures used by Shavlik Technologies for Shavlik Security Suite v8.0. During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Shavlik Security Suite v8.0. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the Shavlik Security Suite v8.0 in its operational environment.

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

12 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The developer's testing approach was to exercise each security function enumerated in the Security Target via the NetChk Protect and NetChk Configure GUIs to demonstrate that the TOE operates as specified. Some tests also required network packet capture and inspection, code inspection and file alteration in order to verify the TOE's self protection mechanisms.

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

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

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. Resulting from this test coverage approach is the following list of DOMUS IT Security Laboratory test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to gain assurance in the developers testing effort by repeating the tests;

b. Audit**.** The objective of this test goal is to verify that the TOE generates audit records each time a machine is scanned, a patch is applied, or a security violation is discovered, and that authorized administrators are able to review the audit records;

c. User Data Protection. The objective of this test goal is to verify the enforcement of role based access control policies and information flow control policies;

d. Identification and Authentication. The objective of this test goal is to verify that the TOE maintains the unique Windows account identifier and assigns a role for each user for access control and auditing purposes;

e. Security Management. The objective of this test goal is to verify the management of security functions, attributes and data as per the developer's design specification;

f. Protection of the TSF. The objective of this test goal is to verify that patch and configuration data is protected from modification while being transmitted between separate parts of the TOE and confirm the invocation and subsequent enforcement of code signing protection mechanisms; and

g. Resource Utilization. The objective of this test goal is to verify that the TOE limits the number of machines that can be scanned simultaneously.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, independent evaluator penetration testing was conducted.

No public vulnerabilities were discovered relating to the TOE. Subsequent to analysis of the developer's evidence, the evaluator focused the penetration tests on bypassing the TOE's security mechanisms and tampering. Direct attack was ruled out as authentication is performed by Windows; monitoring and misuse based vulnerabilities were also ruled out due to the assumptions constraining the environment.

The evaluator performed investigative testing consisting of process and log monitoring to identify weaknesses that may be leveraged to allow the TOE security policy to be violated. The evaluator then postulated and tested a number of attack scenarios focused on accessing local databases, files and registry settings in order to escalate privilege or directly access user data. The evaluator was unable compromise the TOE security policy whilst assuming the role of an attacker with a basic attack potential.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

12.4 Conduct of Testing

Shavlik Security Suite v8.0 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Laboratory, and a Shavlik-hosted virtual environment. 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 a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Shavlik Security Suite v8.0 behaves as specified in its ST and functional specification and TOE design.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ 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 evaluator found Shavlik Security Suite v8.0 to be an intuitive patch and configuration management tool that provides robust security measures. The evaluator recommends that users follow the Shavlik Security Suite v8.0 Guidance Documentation Supplement if they wish to deploy the evaluated configuration. Departure from the evaluated configuration should only be performed in consideration of the deployment scenario and associated risk profile.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
SSI	Shavlik Security Intelligence
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. Shavlik Security Suite v8.0 Security Target, 1.0, 16 June 2010

e. Shavlik Security Suite v8.0 EAL3+ Evaluation Technical Report, v1.1, 16 June 2010