Certification Report

SolarWinds® Log and Event Manager v5.70

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-287-CR
Version: 1.0
Date: 15 October 2014
Pagination: i to iii, 1 to 9

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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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, 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, 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/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 EWA-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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 15 October 2014, 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 trademarks or registered trademarks:

- SolarWinds® is a registered trademark of SolarWinds Worldwide LLC.

TABLE OF CONTENTS

Executive Summary

SolarWinds® Log and Event Manager v5.70 (hereafter referred to as SolarWinds LEM), from SolarWinds Worldwide, LLC, is the Target of Evaluation. The results of this evaluation demonstrate that SolarWinds LEM meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

SolarWinds LEM collects, stores, and normalizes log and event data from a variety of sources, and displays that data in a web interface for monitoring, searching, and analysis. Data is also available for scheduled and ad hoc reporting.

Alerts are created from normalized data that Solarwinds LEM uses to display events/messages from Solarwinds LEM monitored devices. Log data is processed by Solarwinds LEM's policy engine to correlate data based on user defined Rules. These actions can include notifying users, blocking an IP address, shutting down or rebooting a workstation, and passing the alerts on to the Solarwinds LEM database for future analysis and reporting within the Reports application.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 24 September 2014 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 SolarWinds LEM, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the SolarWinds LEM 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

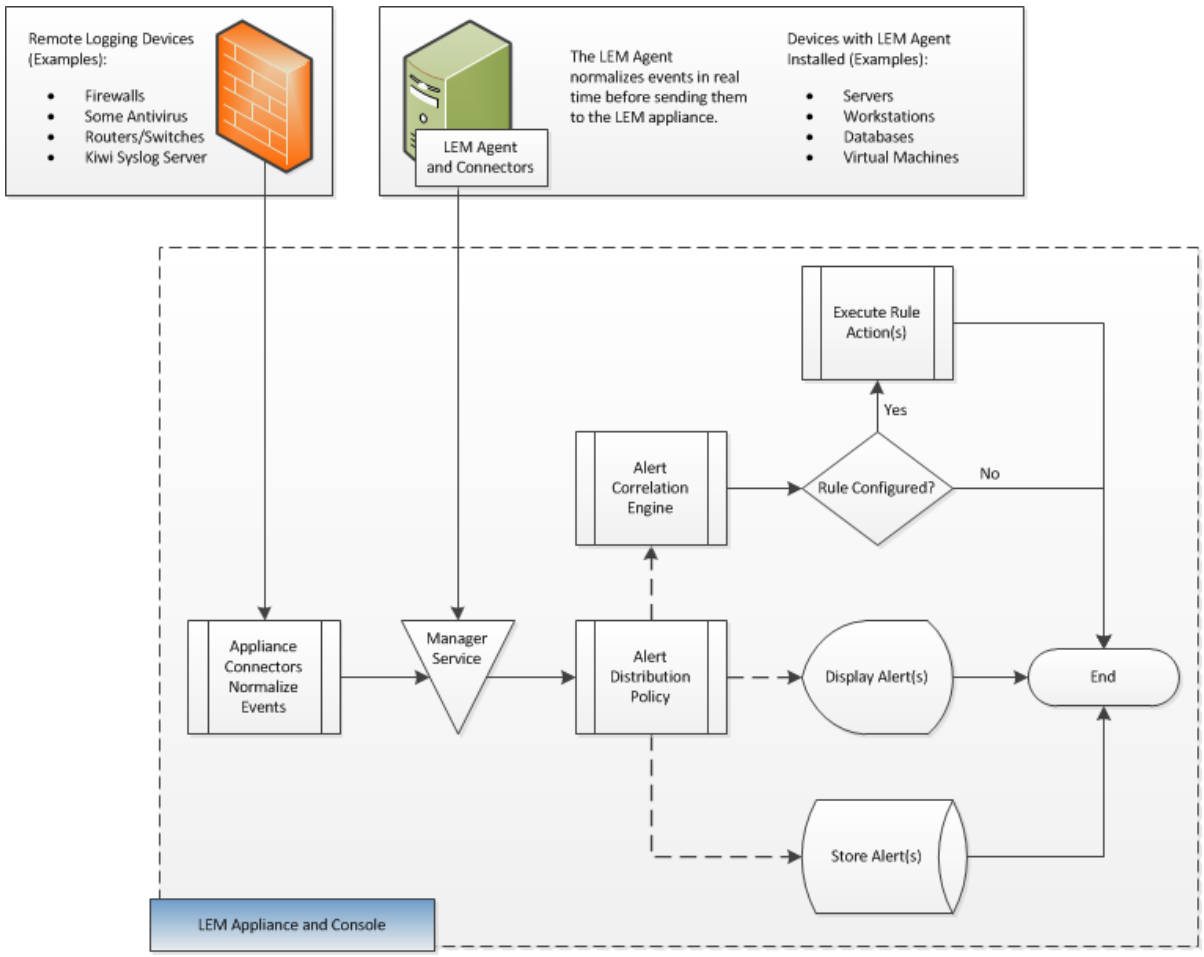
The Target of Evaluation (TOE) for this EAL 2+ evaluation is SolarWinds® Log and Event Manager v5.70 (hereafter referred to as SolarWinds LEM), from SolarWinds Worldwide, LLC.

2 TOE Description

SolarWinds LEM collects, stores, and normalizes log and event data from a variety of sources, and displays that data in a web interface for monitoring, searching, and analysis. Data is also available for scheduled and ad hoc reporting.

Alerts are created from normalized data that Solarwinds LEM uses to display events/messages from Solarwinds LEM monitored devices. Log data is processed by Solarwinds LEM's policy engine to correlate data based on user defined Rules. These actions can include notifying users, blocking an IP address, shutting down or rebooting a workstation, and passing the alerts on to the Solarwinds LEM database for future analysis and reporting within the Reports application.

A diagram of the SolarWinds LEM architecture is as follows:



3 Security Policy

SolarWinds LEM implements a role-based access control policy to control administrative access to the system. In addition, SolarWinds LEM implements policies pertaining to the following security functional classes:

- *Audit;*
- *Identification and Authentication;*
- *Security Management; and*
- *Log and Event Management.*

4 Security Target

The ST associated with this Certification Report is identified below:

SolarWinds® Log and Event Manager Software Security Target version 1.5, 25 August 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

SolarWinds LEM is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
    - ALC_FLR.2 Flaw Reporting Procedures.

b. *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:*
    - FNM_MDC – Monitor Data Collection;
    - FNM_ANL – Monitor Analysis;
    - FNM_RCT – Management React; and
    - FNM_RDR – Restricted Data Review.

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

6 Assumptions and Clarification of Scope

Consumers of SolarWinds LEM 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *The Administrator will install and configure the TOE according to the administrator guidance.*
- *Administrators are non-hostile, competent and on-going, and follow the administrator guidance when using the TOE.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE has access to all the IT System data it needs to perform its functions;*
- *The TOE is appropriately scalable to the IT Systems the TOE monitors;*

- *The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation; and*
- *There will be a network that supports communication between distributed components of the TOE. This network functions properly.*

7 Evaluated Configuration

The evaluated configuration for SolarWinds LEM comprises:

SolarWinds Log And Event Manager v5.7.0, build 9.

Solarwinds LEM is made up of two components:

- The virtual appliance is installed on a virtual platform running VMware vSphere 4, Microsoft Hyper-V 2008 R2, or Microsoft Hyper-V 2012.
- The desktop component is installed on a GPC running one of Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2.

The publication entitled.:

- *SolarWinds Log & Event Manager Common Criteria Supplement, version 1.1, 29 August 2014.*

describes the procedures necessary to install and operate SolarWinds LEM in its evaluated configuration.

8 Documentation

The SolarWinds Worldwide, LLC documents provided to the consumer are as follows:

a. SolarWinds Log & Event Manager Quick Start Guide, version 5.6.6, 6 November 2013;

b. SolarWinds Log & Event Manager User Guide 5.7, 12 October 2013; and

c. SolarWinds Log & Event Manager Common Criteria Supplement, version 1.1, 29 August 2014.

9 Evaluation Analysis Activities

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

Development: The evaluators analyzed the SolarWinds LEM 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 SolarWinds LEM security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that

security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the SolarWinds LEM 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 SolarWinds LEM configuration management system and associated documentation was performed. The evaluators found that the SolarWinds LEM configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of SolarWinds LEM during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the SolarWinds LEM. During a site visit, the evaluators also 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.

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

10 ITS Product Testing

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

10.1 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[1].

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

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

[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.

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 test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured, as identified in the ST, by following the instructions in the developer supplied documentation;

c. Invalid Login Auditing: The objective of this test goal is to confirm that the TOE will log invalid login attempts by an unknown user; and

d. Restrict SSH: The objective of this test goal is to confirm that the TOE will restrict SSH access from an undefined IP address.

10.3 Independent Penetration Testing

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

The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Port Scan: The objective of this test goal is to scan ports using nmap to verify which ports are open;

c. Banner Grabbing: The objective of this test case is to determine if any useful information can be gained from netcat scans of the TOE; and

d. Information Leakage: The objective of this test case is to use a packet capture package to monitor for leakage of sensitive information during login and normal operation of the TOE.

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

10.4 Conduct of Testing

SolarWinds LEM 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 Facility at EWA-Canada. 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.

10.5 Testing Results

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

11 Results of the Evaluation

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

12 Evaluator Comments, Observations and Recommendations

The evaluator recommends that potential operators of the TOE familiarize themselves with the ST and relevant product documentation before operating the appliance. Given that the appliance is installed in a virtual machine environment, it is also required that personnel deploying the SolarWinds Log and Event Manager are properly trained in the operation of the underlying hypervisor.

Care must be taken to ensure that network traffic between the appliance and monitored devices is configured properly. As some features and access to the appliance is controlled solely by IP address it is imperative to the secured operation of the appliance that IT departments control access to these whitelisted devices.

13 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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
LEM	Log and Event Manager
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. SolarWinds® Log and Event Manager Software Security Target version 1.5, 25 August 2014

e. Evaluation Technical Report for SolarWinds® Log and Event Manager Software, version 1.1, 24 September 2014.