National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Lumeta IPsonar 5.5C

Report Number: **CCEVS-VR-VID10506-2013**
Dated: **20 December 2013**
Version: **1.0**

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Incorporated (formerly SAIC)
Columbia, MD

Table of Contents

List of Tables

1. Executive Summary

The evaluation of Lumeta IPsonar 5.5C was performed by Leidos, Inc. (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) located in Columbia, Maryland, United States of America. The evaluation team completed the evaluation in December 2013. The team conducted the evaluation in accordance with the assurance activities defined in *Protection Profile for Network Devices* [9]; the requirements of the *Common Criteria for Information Technology Security Evaluation* [1], [2], [3]; and the evaluator activities in *Common Methodology for Information Technology Security: Evaluation methodology* [4]. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on NIAP's web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is conformant to *Protection Profile for Network Devices* [9]. The information in this Validation report is largely derived from:

- *Evaluation Technical Report for Lumeta IPsonar 5.5C Part 1 (Non-Prop),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013).
- *Evaluation Technical Report for Lumeta IPsonar 5.5C Part 2 (Prop),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013).
- *Assurance Activities Report for Lumeta IPsonar 5.5C,* Version 1.0, 9 October 2013 (with ECR Addendum 19 December 2013).
- *Evaluation Team Test Report for Lumeta IPsonar 5.5C,* Leidos (formerly SAIC) CCTL, version 1.0, 9 October 2013 (with ECR Addendum 19 December 2013)

This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. Government, and no warranty is either expressed or implied.

The product, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in *Protection Profile for Network Devices* [8].

1.1 Evaluation Details

Table 1 provides information needed to completely identify the product.

Table 1 – Evaluation Details

Evaluated Product:	Lumeta IPsonar 5.5C
Sponsor:	Lumeta Corporation
Developer:	Lumeta Corporation
CCTL:	Leidos Incorporated (formerly Science Applications International Corporation) Common Criteria Testing Laboratory

VALIDATION REPORT

Lumeta IPsonar 5.5C

6841 Benjamin Franklin Drive

Columbia, MD 21046

Kickoff Date:	June 20, 2012
Completion Date:	December 19, 2013
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3, July 2009
Evaluation Class:	Network Device
Description:	The Target of Evaluation (TOE) is a network device that provides a secure base for its other operational functions, primarily involving auditing, cryptographic support (for network communication and update integrity), user identification and authentication, secure management, and secure product updates. The product is designed to plug into a network and to actively examine and discover the network infrastructure. To that end it can identify and examine network connected assets such as hosts and other network devices in order to create a view of the routed infrastructure associated with the attached network.
Disclaimer:	The information contained in this Validation Report is not an endorsement of Lumeta IPsonar 5.5C product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	*Protection Profile for Network Devices*, Version 1.1, 8 June 2012
Evaluation Personnel:	Leidos (formerly SAIC): Gary Grainger Christopher Keenan Eve Pierre
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

1.4 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE is intended to meet:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

1.5 Clarification of Scope

Note that while the TOE provides network discovery capability as the primary function of the TOE, the implementation and correct operation of those functions was outside the scope of the evaluation. The scope of the evaluation did not include any functionality not specifically addressed in the security requirements. The evaluation focused on the security of the device as a network infrastructure component as required in the the *Protection Profile for Network Devices* [8].

2. Identification

The evaluated product is Lumeta IPsonar 5.5C (Report/Scan server version: 5.5.0.12174101C; Sensor version: 5.5.3.12338104). The TOE is the whole product.

3. Security Policy

The TOE enforces the following security policies as described in the ST.

3.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE uses FreeBSD-based auditing features that can be configured to store the logs locally so they can be accessed by an administrator and also sent to a remote log server using syslog-ng in order to protect the exported records using TLS.

3.2 Cryptographic support

The TOE includes the FIPS-certified OpenSSL FIPS Object Module (FIPS 140-2 Cert. #1051) (valid on compatible operating systems along with CAVP algorithm testing specific to IPsonar 5.5) that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS/HTTPS.

3.3 User data protection

The TOE performs a variety of network infrastructure detection functions, but as a rule does not pass data among network entities. The exception is that data is passed among distributed TOE appliances. Otherwise, it collects data from the network and attached components and ultimately forwards information to TOE administrators.

Regardless, the TOE is designed to ensure that memory and other storage resources are reused properly to mitigate potential data corruption or repetition.

3.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE. It provides the ability to both assign attributes (user names, passwords and roles/privilege levels) and to authenticate users against these attributes. Users can optionally be configured with public certificates so that PKI-based authentication can be used.

3.5 Security management

The TOE provides menu-driven console (Console) commands and a Web-based Graphical User Interface (Web GUI) to access the wide range of security management functions to manage its security policies. Security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are

controlled through the use of privileges associated with roles that can be assigned to TOE users.

3.6 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and private cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). Note that the TOE is a single appliance or an associated collection of appliances acting together. The communication between associated appliances is protected using TLS. The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

3.7 TOE access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

3.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for Console access or TLS/HTTPS for Web graphical user interface access. In each case, both integrity and disclosure protection are ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with an audit log server using TLS connections as part of a syslog-ng implementation to prevent unintended disclosure or modification of logs.

4. Assumptions

The ST identifies the following assumptions about the use of the TOE and its operational environment:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5. Architectural Information

The TOE can be deployed as a single stand-alone appliance or as a collection of cooperating appliances. In the latter case some of the appliances are configured to provide only a subset of the overall functions of the IPsonar appliance. The following list summarizes the modes of operation available within each IPsonar appliance:

- **Sensors.** Network scanning is achieved through the use of network entry points called Sensors. The TOE can be deployed as a Sensor so that it can collect information about its connected network and forward that information to a configured Scan Server.
- **Scan Servers.** These Scan Servers are positioned at appropriate points in the network to ensure connectivity with any distributed Sensors. Multiple scans can be run simultaneously by using multiple configured Sensors.
- **Report Servers.** Functioning as the data repository, Report Servers separate report generation from scanning to reduce IPsonar's operational footprint. A single remote Report Server can support multiple configured Scan Servers.

Physically, the TOE consists of one or more physical appliances (identified above). Each appliance can be deployed in one of three main configurations: Network Sensor, Network Sensor/Scan Server, or Network Sensor/Scan Server/Report Server. Each appliance includes physical network connections allowing access to the subject networks, communication among associated appliances, and remote access by administrators.

6. Documentation

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- *Access Accountability: Managing Console Login Accounts,* Lumeta Corporation, document reference IP_TN_Accountability, revision 3, 4 December 2012
- *IPsonar Common Criteria Guide,* Document Reference IP_CommonCriteriaGuide, revision 1.0, 18 December 2013
- *IPsonar Administrator Guide,* Lumeta Corporation, Document Reference IP_55_AG, version 1, 19 December 2013
- *Format of Syslog Events in IPsonar,* Lumeta Corporation, IP_FOSE_AG_supplement, revised 12/18/2013

Any other guidance documentation provided in hard-copy or electronically with the product was not part of the evaluation.

7. Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Evaluation Team Test Report for Lumeta IPsonar 5.5C,* Version 1.0, 7 October 2013.

7.1 Developer Testing

The assurance activities in *Protection Profile for Network Devices* do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

Evaluation team testing was conducted at Lumeta Facilities in Somerset, NJ.[1]

The evaluation team devised a Test Plan based on the testing assurance activities specified *Protection Profile for Network Devices.* The Test Plan describes how the team was to perform each test activity in the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in *Evaluation Team Test Report for Lumeta IPsonar 5.5C.* The evaluation team tested both TOE platforms (laptop and rack-mounted appliances).

Testing demonstrated the TOE satisfies the security functional requirements specified in the protection profile.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerability applicable to the TOE in its evaluated configuration.

The evaluation team performed a port scan of each TOE. The scan results show the only open ports were for TOE operation.

Lumeta product literature describes an application programming interface to non-security functions of the product. The evaluation team confirmed the TOE requires a user to authenticate before granting access to the interface.

8. Evaluated Configuration

The TOE is the Lumeta IPsonar 5.5 running on FreeBSD-8.1 operating system. The OS is an integral part of the product and is not managed separately (even for upgrades, which Lumeta provides). The TOE can be deployed as a standalone appliance or alternately as a series of cooperating appliances depending on the specific needs of the user.

The TOE is available as either a 1U rack-mountable appliance or alternately as a preconfigured laptop. The hardware is commodity computers running x86 64-bit compatible CPU. The specific hardware tested is Dell d1950 PowerEdge and HP ProBook 6555b. The same security and functional capabilities are available regardless of the physical form factor.

Note that the use of the following features is limited in the evaluated TOE:

1) The TOE provides default user accounts for access to the console. These user accounts enable anonymous logins to the TOE. Anonymous logins are not permitted

[1] The evaluation team accessed the TOE remotely to execute a few follow-up tests.

in the evaluated configuration and must be disabled. During configuration, Authorized Administrators must create password-controlled logins for TOE users to access the console. These user accounts replace the pre-configured anonymous accounts. Once the procedures for configuring the new user accounts have been followed, anonymous logins are disabled.

2) The evaluated configuration requires these additional elements:
   a) The TOE must be configured to operate in FIPS mode. This configuration is performed prior to shipment of the TOE to the customer and cannot be changed. The TOE does not offer the ability to change the FIPS mode configuration and there are no commands availability to modify the FIPS settings.
   b) The Authorized Administrator must follow the instructions provided in Appendix A of the IPsonar Administrator Guide (IP_55CC_AG.docx) for configuring the TOE into the evaluated configuration. This includes performing additional settings such as enabling the Secure System mode by running the secure_system.sh command; enabling the password controls; and creating the replacement users as described above.

The SFTP feature in IPsonar to upload certain prior saved data is not in the scope of this evaluation.

To use the product in the evaluated configuration, the product must be configured as specified in Lumeta's guidance documentation:

- *IPsonar Administrator Guide*, Lumeta Corporation, Document Reference IP_55_AG, version 1, 4 December 2012
- *Access Accountability: Managing Console Login Accounts*, Lumeta Corporation, document reference IP_TN_Accountability, revision 3, 4 December 2012

9. Results of the Evaluation

The results of the security assurance requirements and protection profile assurance activities are summarized in this section. The evaluation team documented the results in detail in:

- *Evaluation Technical Report for Lumeta IPsonar 5.5C Part 1 (nonProp),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013),
- *Evaluation Technical Report for Lumeta IPsonar 5.5C Part 2 (Prop),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013) and
- *Assurance Activities Report for Lumeta IPsonar 5.5C,* Version 1.0, 9 October 2013 (with ECR Addendum 19 December 2013).

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Part 2 to ETR, *Evaluation Technical Report for Lumeta IPsonar 5.5C Part 2 (Prop),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013).

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon the assurance activities specified in the *Protection Profile for Network Devices*, CC version 3.1 Revision 3, and CEM version 3.1 Revision 3. The evaluation team performed each assurance activity in the protection profile. In conjunction with the assurance activities, the evaluation team completed CEM work units for the profile security assurance requirements. The evaluation determined the TOE satisfies the conformance claims made in *Lumeta IPsonar Security Target*. The TOE conforms to the requirements specified in *Protection Profile for Network Devices*.

The rationale supporting each CEM work unit verdict is recorded in *Evaluation Technical Report for Lumeta IPsonar 5.5C Part 2 (Prop)*, which is considered proprietary.

9.1 Evaluation of the Security Target (ASE)

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a statement of security objectives for the TOE, a statement of security requirements claimed to be met by the TOE that are consistent with *Protection Profile for Network Devices*, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation Team performed the TSS assurance activities specified in *Protection Profile for Network Devices* and completed each CEM work unit for each ADV requirement in the profile. The Evaluation Team assessed the evaluation evidence and found it adequate to meet the requirements specified in the PP for design descriptions. The evidence consists of the Security Target and the guidance documentation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the assurance activities and CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation Team performed the TSS assurance activities specified in *Protection Profile for Network Devices* and completed each CEM work unit for each AGD requirement in the profile. The Evaluation Team assessed the evaluation evidence and found it adequate to meet the requirements specified in the protection profile for guidance descriptions. The Evaluation Team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The Evaluation Team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the

evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the assurance activities and CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life-cycle Support (ALC)

The Evaluation Team performed the TSS assurance activities specified in *Protection Profile for Network Devices* and completed each CEM work unit for each ALC requirement in the profile in accordance with the protection profile. The Evaluation Team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The Evaluation Team performed the TSS assurance activities specified in the *Protection Profile for Network Devices* and completed each CEM work unit for each ATE requirement in the profile. The Evaluation Team ensured that the TOE performed as described in the evaluation evidence and demonstrated that the TOE passes the tests specified in the PP.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that evaluator activities addressed the test activities in the protection profile, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The Evaluation Team performed the TSS assurance activities specified in the *Protection Profile for Network Devices* and completed each CEM work unit for each AVA requirement in the profile. The Evaluation Team performed a search of public domain sources of information for possible vulnerabilities in the TOE. The search identified no obvious vulnerability in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis assurance activities in the protection profile, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the PP. Additionally, the Evaluation Team's performance of tests also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the protection profile, and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

The user is cautioned to review the all the administrative guidance when configuring the device into the Common Criteria evaluated configuration, including the instructions provided in Appendix A of the IPsonar Administrator Guide (IP_55CC_AG.docx) as well as the IPsonar Common Criteria Guide Rev 1, December 18, 2013.

11. Security Target

The security target for the evaluation is *Lumeta IPsonar Security Target,* Version 1.0, 7 October 2013.

12. Bibliography

[1] *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model,* Version 3.1, Revision 3, July 2009, CCMB-2009-07-001.

[2] *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components,* Version 3.1, Revision 3, July 2009, CCMB-2009-07-002.

[3] *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components,* Version 3.1, Revision 3, July 2009, CCMB-2009-07-003.

[4] *Common Methodology for Information Technology Security: Evaluation methodology,* Version 3.1, Revision 3, July 2009, CCMB-2009-07-004.

[5] *Evaluation Technical Report for Lumeta IPsonar 5.5 Part 1 (Non-Prop),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013).

[6] *Evaluation Technical Report for Lumeta IPsonar Part 2 (Prop),* Version 1.0, 9 October 2013 (with ECR update 19 December 2013).

[7] *Assurance Activities Report for Lumeta IPsonar 5.5C,* Version 1.0, 9 October 2013 (with ECR Addendum 19 December 2013).

[8] *Evaluation Team Test Report for Lumeta IPsonar 5.5C,* Leidos (formerly SAIC) CCTL, version 1.0, 9 October 2013 (with ECR Addendum 19 December 2013)

[9] *Protection Profile for Network Devices,* Version 1.1, 8 June 2012.

[10] *Lumeta IPsonar Security Target,* Version 1.0, 7 October 2013.

[11] *Access Accountability: Managing Console Login Accounts,* Lumeta Corporation, document reference IP_TN_Accountability, revision 3, 4 December 2012

[12] *IPsonar Administrator Guide,* Lumeta Corporation, Document Reference IP_55_AG, version 1, 4 December 2012

[13] *Format of Syslog Events in IPsonar,* Lumeta Corporation, IP_FOSE_AG_supplement, revised 8/15/2013

[14] *IPsonar Common Criteria Guide,* Lumeta Corporation, Document Reference IP_CommonCriteriaGuide, revision 1.0, 18 December 2013