# Certification Report

## Violin Memory 6000 Series Memory Arrays with Memory Gateways Version 5.5.2

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**



**Document number**: 383-4-266-CR
**Version**: 1.0
**Date**: 4 July 2014
**Pagination**: i to iii, 1 to 8

# 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 4 July 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:

- Violin Memory is a registered trademark of Violin Memory, Inc.

**TABLE OF CONTENTS**

## Executive Summary

Violin Memory 6000 Series Memory Arrays with Memory Gateways Version 5.5.2 (hereafter referred to as Violin Memory 6000 Series), from Violin Memory, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Violin Memory 6000 Series meets the requirements of Evaluation Assurance Level (EAL) 2+ for the evaluated security functionality.

Violin Memory 6000 Series are stand-alone purpose-built memory arrays. The Violin Memory 6000 Series enables thousands of flash devices to operate efficiently as a flash memory array and are intended for any application that requires active processing or rapid access to large amounts of data. The flash memory may be configured as multiple Logical Unit Numbers (LUNs) and accessed from the servers using standard block access transport protocols over the Storage Area Network (SAN). Access to individual LUNs may be restricted by authorized administrators to a LUN-specific list of servers.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 12 May 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 Violin Memory 6000 Series, 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 Violin Memory 6000 Series 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).

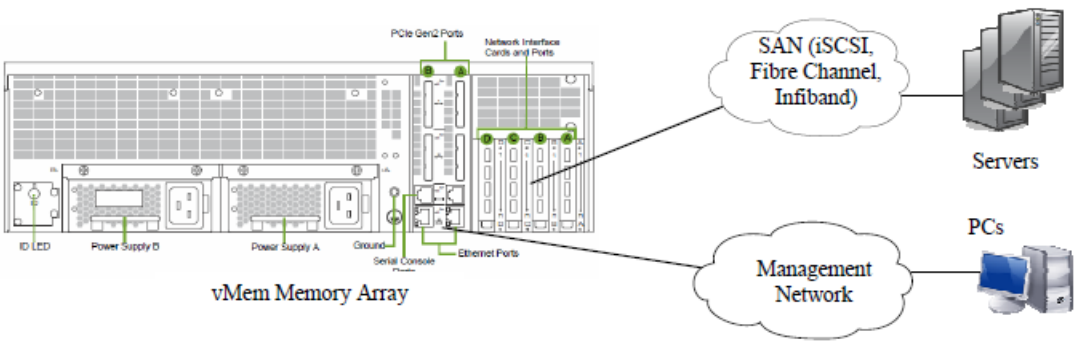
# 1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2 + evaluation is Violin Memory 6000 Series Memory Arrays with Memory Gateways Version 5.5.2 (hereafter referred to as Violin Memory 6000 Series), from Violin Memory, Inc.

# 2 TOE Description

Violin Memory 6000 Series are stand-alone purpose-built memory arrays. The Violin Memory 6000 Series enables thousands of flash devices to operate efficiently as a flash memory array and are intended for any application that requires active processing or rapid access to large amounts of data. The flash memory may be configured as multiple Logical Unit Numbers (LUNs) and accessed from the servers using standard block access transport protocols over the Storage Area Network (SAN). Access to individual LUNs may be restricted by authorized administrators to a LUN-specific list of servers.

A diagram of the Violin Memory 6000 Series architecture is as follows;



# 3 Security Policy

Violin Memory 6000 Series implements a role-based access control policy to control administrative access to the system. In addition, Violin Memory 6000 Series implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *Security Management;*
- *User Data Protection; and*
- *Identification and Authentication.*

# 4 Security Target

The ST associated with this Certification Report is identified below:

Violin Memory 6000 Series Memory Arrays with Memory Gateways Security Target, Version 1.7, 4 March 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.*

Violin Memory 6000 Series is:

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

b. *Common Criteria Part 2 conformant; with security functional requirements based only upon functional components in Part 2.*

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 Violin Memory 6000 Series 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:

- *There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains; and*
- *The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.*

### 6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users; and*
- *The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.*

## 7 Evaluated Configuration

The evaluated configuration for Violin Memory 6000 Series comprises one of the following appliance models:

- 6606;
- 6611;
- 6616;
- 6212;
- 6222; and
- 6232.

Each model has the following software pre-installed:

- vMOS software, which is Violin Memory 6000 Series Memory Arrays with memory Gateways Version 5.5.2 build number 1, executes on the array controllers; and
- vSHARE software, which is Violin Memory 6000 Series Memory Arrays with memory Gateways Version 5.5.2 build number 7, executes on the Memory Gateways.

These models all provide the same security functionality; they differ in throughput, flash type and flash capacity only.

The publications entitled

- *Violin Memory 6000 Series Memory Array Installation Guide For Release A5.5.2 and G5.5.2; and*
- *Violin Memory Arrays Version 5.5.2 Common Criteria Supplement.*

describes the procedures necessary to install and operate Violin Memory 6000 Series in its evaluated configuration.

## 8 Documentation

The Violin Memory, Inc. documents provided to the consumer are as follows:

- *Violin Memory 6000 Series Memory Array Installation Guide For Release A5.5.2 and G5.5.2;*

- *Violin Memory 6000 Series Memory Array User's Guide For Release A5.5.2 and G5.5.2; and*
- *Violin Memory Arrays Version 5.5.2 Common Criteria Supplement.*

# 9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Violin Memory 6000 Series, including the following areas:

**Development:** The evaluators analyzed the Violin Memory 6000 Series functional specification and determined that the functional specification and TOE design describes the purpose and method of use for each TSF interface and that the Violin Memory 6000 Series functional specification is an accurate and complete instantiation of the SFRs.

**Guidance Documents:** The evaluators examined the Violin Memory 6000 Series 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 Violin Memory 6000 Series configuration management system and associated documentation was performed. The evaluators found that the Violin Memory 6000 Series 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 Violin Memory 6000 Series during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Violin Memory 6000 Series. 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].

[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.

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.

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. Initialization, verification and configuration: the objective of this test goal is to ensure that the TOE is correctly initialized, verified and configured prior to the start of functional testing;

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

c. Concurrent Login Behaviour and Login: The objective of this test goal is to demonstrate the TOE's concurrent login behaviour, and associated user identification and authorization, management of user accounts and security management;

d. Security Roles, TSF Data and User-Subject binding: The objective of this test case is to demonstrate the management of security roles and TSF Data and user-subject binding; and

e. Session Inactivity termination: The objective of this test goal is to demonstrate TOE session inactivity termination.

### 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. Banner Grabbing: The objective of this test goal is to determine if any useful information can be gained from the Memory Gateway IP or the Array Controller Module Management IP of Violin Memory; and

c. Heartbleed exploitation: The objective of this test goal is to determine if the TOE is vulnerable to the OpenSSL Heartbleed exploit and attempt to compromise the TOE using it.

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

### 10.4 Conduct of Testing

Violin Memory 6000 Series 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. 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 Violin Memory 6000 Series 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

It is recommended that once the TOE is powered on, it remain powered on, and be operated on a Uninterruptable Power Supply, and in an air-conditioned environment with good airflow around the TOE

# 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 |
| GB Gigabyte | |
| IT | Information Technology |
| LUN | Logical Unit Number |
| PALCAN | Program for the Accreditation of Laboratories - Canada |
| SAN | Storage Area Network |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TB | Terabyte |
| 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. Violin Memory 6000 Series Memory Arrays with Memory Gateways Security Target, Version 1.7, 4 March 2014

e. Evaluation Technical Report for Violin Memory, Inc Violin Memory 6000 Series Memory Arrays with Memory Gateways, v1.0, 12 May 2014.