Certification Report

EAL 3 Evaluation of Citadel Security Software Inc.

Hercules® Enterprise Vulnerability Management (EVM) Version 4.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© 2006 Government of Canada, Communications Security Establishment

Document number: 383-4-47-CR
Version: 1.0
Date: 23 October 2006
Pagination: i to v, 1 to 13

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 2.2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.2*. 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 (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 Electronic 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 23 October 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 or registered trademarks:

- Hercules is a registered trademark of Citadel Security Software Inc in the United States.
- Microsoft, Windows, Windows NT, Windows Server, and SQL Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- CVE is a trademark of MITRE Corporation.
- HP-UX is a trademark of Hewlett Packard Company in the United States.
- Intel and Pentium are registered trademarks of Intel.
- Linux is a registered trademark of Linus Torvalds. Inc..
- Mac OS X is a registered trademark of Apple Computer, Inc..
- Red Hat is a registered trademark of Red Hat, Inc..
- SANS is a trademark of SANS/ESCAL.
- Cisco IOS, Cisco CATOS, Cisco VPN, Cisco PIX, either are trademarks or registered trademarks of Cisco Systems Inc. and its affiliates in the United States and other countries.
- Sun and Solaris are trademarks of Sun Microsystems, Inc. in the United States and other countries.
- UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd..
- AIX is a registered trademark of International Business Machines Corporation.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The Hercules® Enterprise Vulnerability Management (EVM) v4.1, from Citadel Security Software Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

The Hercules® EVM is designed to facilitate the automatic vulnerability remediation of devices on large-scale enterprise level Windows®, Mac OS X®, and Unix (AIX®/HP-UX®/Solaris™/Linux®) based networks. The product imports vulnerability information from a number of third party commercial vulnerability scanner products and consolidates this information into a single view of the vulnerabilities of each device on the network. The product provides a sequence of automatically executable remediation steps to correct each recognized vulnerability. Users of the product may download new signatures from the V-Flash server operated by Citadel Security Software. The Hercules® EVM provides an interface which allows users to view the listed vulnerabilities of devices on the network. Logical groupings of devices may be defined. An automatic remediation schedule may be defined for a group. In addition, a specific list of vulnerabilities to be remediated, known as a remediation profile, may be defined for the group.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed 17 October 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 Hercules® EVM, 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 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

CSE, as the CCS Certification Body, declares that the Hercules® EVM 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) at http://www.cse-

[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.

cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation is the Hercules® Enterprise Vulnerability Management (EVM) v4.1, from Citadel Security Software Incorporated.

2 TOE Description

The Hercules® EVM is designed to facilitate the automatic vulnerability remediation of devices on large-scale enterprise level Windows®, Mac OS X®, and Unix (AIX®/HP-UX®/Solaris™/Linux®) based networks. The product imports vulnerability information from a number of third party commercial vulnerability scanner products and consolidates this information into a single view of the vulnerabilities of each device on the network. The product provides a sequence of automatically executable remediation steps to correct each recognized vulnerability. Users of the product may download new signatures from the V-Flash server operated by Citadel Security Software. The Hercules® EVM provides an interface which allows users to view the listed vulnerabilities of devices on the network. Logical groupings of devices may be defined. An automatic remediation schedule may be defined for a group. In addition, a specific list of vulnerabilities to be remediated, known as a remediation profile, may be defined for the group.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Hercules® EVM can be found 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: Security Target Citadel Hercules® Enterprise Vulnerability Management (EVM) Version 4.1
Revision: 1.1
Date: 3 August 2006

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2*.

The Hercules® Enterprise Vulnerability Management (EVM) v4.1 is:

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

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 3 conformant, with all the security assurance requirements in the EAL 3 package.

6 Security Policy

The Hercules® EVM implements role based access control and information flow control policies to control user access to system resources and to control the flow of vulnerability and remediation data through the system. Policy detail can be found in section 5.4 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Hercules® EVM 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

Personnel authorized to install, configure, and operate the Hercules® EVM possess appropriate training and will adhere to the procedures for secure usage of the product.

Personnel authorized to install, configure, and operate the Hercules® EVM will adhere to all organizational policies including standards regarding secure usage of computer resources including physical, network, and password security policies.

The organization operating the Hercules® EVM has backup and recovery procedures in place such that the Hercules® EVM may be recovered to a secure configuration if a hardware failure were to occur.

The Administrator enforces all organizational password security policies when assigning credentials to users.

Organizational role-based access control policies are in place that determine which individuals are authorized Hercules® EVM users, and the privileges associated with each such user.

7.2 Environmental Assumptions

The host machine upon which the Hercules® EVM is installed resides in a physically secure location and only authorized individuals are granted physical access to the host.

The host operating system upon which the Hercules® EVM resides has been installed, configured and security-hardened in accordance with the *Hercules® Security Configuration Guide, Document Version 1.1, May 2006*.

For more information about the TOE security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

The Hercules® EVM cannot prevent authorized administrators from carelessly configuring or using the Hercules® EVM such that network protection is compromised.

8 Architectural Information

The Hercules® EVM is a software product comprising the following main components:

Hercules® EVM Administrator Console. The Hercules® EVM Administrator Console provides the user interface for the product and includes the display and input devices through which the user interacts with the Hercules® EVM application. The EVM Console uses SSL-based communications with the Hercules® EVM Server(s), and has the ability to interact with Windows® user accounts, domain privileges and NTFS privileges. It authenticates (using Windows® integrated authentication) to the Internet Information Server (IIS) on the Hercules® EVM Server. The EVM Console is designed to be installed and used on a trusted and appropriately configured and controlled Windows® machine that is used for network administration.

Hercules® EVM Server. The Hercules® EVM Server comprises a Hercules® SQL Server, Hercules® File Download Server, and Hercules® Channel Server, and communicates with the Hercules® EVM Clients to distribute remediation profiles and gather remediation progress data. Multiple EVM Servers may be deployed within a network and administered from a single Administrator Console. The EVM Server is designed to be installed and used on a trusted and appropriately configured and controlled Windows® server.

Hercules® EVM Windows®, Unix®, and Mac® Clients. The Hercules® EVM Windows®, Unix®, and Mac® Clients are services that perform remediation activities on network devices such as workstations and servers. The clients establish HTTPS/SSL-based communication to the Hercules® EVM Server.

9 Evaluated Configuration

The Hercules® EVM includes three evaluated configurations: Standalone; Appliance; and Distributed. The three configurations comprise the same functional components and differ only in packaging. The three configurations are described in detail in the ST Sections 2.1.2, 2.1.3, and 2.1.4 respectively.

9.1 Standalone configuration

9.1.1 A Hercules® EVM Administrator Console executing on an Intel® Pentium based PC running one of the following operating systems:

- Windows® 2000 Server with Service Pack 4;

- Windows® 2000 Advanced Server with Service Pack 4;
- Windows 2000 Professional with Service Pack 4, Windows® XP Professional with Service Pack 2;
- Windows® Server 2003 Standard Edition; or
- Windows® Server 2003 Enterprise Edition.

The following software is also required for all configurations:

- Internet Explorer 5.5 or higher;
- Microsoft .NET Framework v1.1; and
- Adobe Acrobat Reader™ 5.0 or higher.

9.1.2 One or more Hercules® EVM Server(s) executing on an Intel® Pentium based PC running one of the following operating systems:

- Windows® 2000 Server with Service Pack 4;
- Windows® 2000 Advanced Server with Service Pack 4;
- Windows® Server 2003 Standard Edition; or
- Windows® Server 2003 Enterprise Edition.

For the Windows® 2000 Server family, IIS 5.0 is required, and for the Windows® Server 2003 family, IIS 6.0 is required.

The following software is also required for all configurations:

- Internet Explorer 6.0 with service pack 1;
- Adobe Acrobat Reader™ 5.0 or higher;
- Microsoft SQL Server 2000 SP3A;
- Microsoft Reporting Services SP1;
- Microsoft .NET Framework v1.1; and
- Microsoft ASP.Net.

9.1.3 One or more network devices with Hercules® EVM Client Version 4.1 installed on either a supported Windows®, UNIX®, or Mac® operating system.

Windows® operating system

The supported Windows® operating systems are:

- Windows® NT 4.0 Workstation with Service Pack 6;
- Windows® NT 4.0 Standard Server with Service Pack 6
- Windows® NT 4.0 Terminal Server with Service Pack 6;
- Windows® 2000 Professional with any service pack;
- Windows® 2000 Server with any service pack;
- Windows® 2000 Advanced Server with any service pack;
- Windows® XP Professional with any service pack;
- Windows® Server 2003 Standard Edition;
- Windows® Server 2003 Small Business Edition;
- Windows® Server 2003 Web Edition; and
- Windows® Server 2003 Enterprise Edition.

For Windows® NT 4.0 platforms, Internet Explorer 5.5 with service pack 2 or above is also required.

UNIX® operating system

The supported UNIX® operating systems are:

- Solaris™ versions 2.6, 7, 8, 9, and 10;
- Linux Red Hat® versions 7.3, 8, 9, 2.1 (AS, ES, WS), 3(AS, ES, WS), 4 (AS, ES, WS);
- AIX® versions 5.1, 5.2, 5.3;
- HP-UX® versions 11.0, 11i v1; and
- Tru64® 5.1B.

The following software is also required for all configurations:

- Open SSH v3.5p1 or higher;
- Open SSL 0.96 or higher; and
- Sudo v1.6.7 or higher.

Mac® operating system

The supported Mac® operating systems are Mac OS X 10.2, 10.3, and 10.4.
The following software is also required for all configurations:

- Open SSH v3.5p1 or higher;
- SSL/HTTPS enabled with Open SSL 0.96 or higher; and
- Sudo v1.6.7 or higher.

9.2 Appliance configuration

The Hercules® EVM Appliance configuration is identical to the standalone configuration and operates on the Windows® Server 2003 operating system with integrated Microsoft SQL Server. The only difference is that Citadel provides the hardware as well as the software. This results in a standalone package that may be conveniently inserted into an existing network with minimal configuration on the customer's part. The product identification is SYS-G-CIT100-000, where SYS-G-CIT100 represents the appliance model, and the minor number (000) can be used to signify additional configuration options such as hard drive size and memory.

9.3 Distributed configuration

In the distributed configuration, the Hercules® Channel Server and the Hercules® Download Server may be installed separately from the Hercules® SQL Server. The Hercules® Channel Server and the Hercules® Download Server have the same operating system support requirements as the Hercules® SQL Server.

10 Documentation

The Citadel Security Software Inc. documents provided to the consumer are as follows:

- Hercules® Installation Guide;
- Hercules® QuickStart Guide;

- Hercules® Remedy Actions Reference;
- Hercules® Reporting Schema;
- Hercules® Security Configuration Guide;
- Hercules® User's Guide;
- Hercules® Vulnerability Assessment and Remediation Overview; and
- Creating Network Install Package for Microsoft Internet Explorer 6.0.

These documents are provided in Adobe PDF format on the shipped CD.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Hercules® EVM, including the following areas:

Configuration management: An analysis of the Hercules® EVM development environment and associated documentation was performed. The evaluators found that the Hercules® EVM 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 Hercules® EVM 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 Hercules® EVM 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 Hercules® EVM user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development

environment to protect the confidentiality and integrity of the Hercules® EVM design and implementation.

Vulnerability assessment: The strength of function claims in the ST were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the Hercules® EVM 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. Penetration testing was conducted by evaluators, which did not expose any residual vulnerabilities that would be exploitable in the intended operating environment for the TOE.

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

12 ITS Product Testing

Testing consists of the following three areas: coverage, functional tests, independent testing. The evaluators examined the developer's testing activities and verified that the developer has met their testing responsibilities.

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].

Citadel employs a rigorous testing process that tests the changes and fixes in each release of the Hercules® EVM. Comprehensive regression testing is conducted for all releases.

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 was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluators 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 focussed on:

[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.

- Identification and Authentication;
- Audit;
- Users and Roles; and
- User Data Protection.

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 Hercules® EVM in the anticipated operating environment.

12.4 Conduct of Testing

The Hercules® EVM was subjected to a comprehensive suite of formally documented independent functional tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at Electronic 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 ETR.

12.5 Testing Results

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

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 complete documentation for the Hercules® EVM includes a comprehensive Installation and Security Guide and a User's Guide.

The Hercules® EVM is straightforward to configure, use and integrate into a corporate network.

Citadel Security Software Inc. Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

15 Glossary

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

15.1 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
CSE	Communications Security Establishment
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVM	Enterprise Vulnerability Management
HTTPS	Hyper Text Transfer Protocol Secure Sockets
IIS	Internet Information Server
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NTFS	New Technology File System
OS	Operating System
PDF	Postscript Document Format
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SANS	SysAdmin, Audit, Network, Security
SFP	Security Function Policy
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.2 Revision 326, December 2004.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.2 Revision 326, December 2004.

d. Security Target Citadel Hercules® Enterprise Vulnerability Management (EVM) Version 4.1, Revision No. 1.1, 3 August 2006.

e. Evaluation Technical Report (ETR) Hercules® Enterprise Vulnerability Management v4.1, EAL 3 Evaluation, Common Criteria Evaluation Number: 383-4-47, Document No. 1517-000-D002, Version 0.3, 27 September 2006.