Certification Report

EAL 3 Evaluation of Citadel Security Software, Inc.

Hercules® Automated Vulnerability Remediation (AVR)

Version 2.2.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-18
Version: 1.1
Date: 1 March 2004
Pagination: i to v, 1 to 17

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 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.1*. 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 1 March 2004, 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 at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names:

a. Hercules which is a trademark of Citadel Security Software, Inc.;

b. Microsoft, Internet Explorer, Windows Server 2003, Windows 2000 Server, Windows 2000 Advanced Server, and Windows XP which are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries;

c. Red Hat, which is a trademark of Red Hat, Inc.;

d. "CERT" and "CERT Coordination Center" are registered with the U.S. Patent and Trademark office as service marks of Carnegie Mellon University. When you refer to the CERT/CC in writing, please use "the CERT® Coordination Center" or "the CERT®/CC." You should not expand "CERT" into an acronym; but it is appropriate to note in your text that the CERT/CC was the first computer security incident response team.

e. Sun and Solaris, which are trademarks of Sun Microsystems, Inc.; and

f. Intel, which is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **3**

2 TOE Description **3**

3 Evaluated Security Functionality **4**

4 Security Target **4**

5 Common Criteria Conformance **4**

6 Security Policy **4**

6.1 INFORMATION FLOW CONTROL SECURITY FUNCTIONAL POLICY HERCULES® AVR SERVER TO CLIENT [SERVER_SFP] 4
6.2 INFORMATION FLOW CONTROL SECURITY FUNCTIONAL POLICY VULNERABILITY SCANNER IMPORT [IMPORT_SFP] 5

7 Assumptions and Clarification of Scope **5**

7.1 SECURE USAGE ASSUMPTIONS 5
7.2 ENVIRONMENTAL ASSUMPTIONS 6
7.3 CLARIFICATION OF SCOPE 6

8 Architectural Information **6**

9 Evaluated Configuration **7**

10 Documentation **8**

11 Evaluation Analysis Activities **9**

12 ITS Product Testing **10**

12.1 ASSESSING DEVELOPER TESTS 10
12.2 INDEPENDENT FUNCTIONAL TESTING 10
12.3 INDEPENDENT PENETRATION TESTING 13
12.4 CONDUCT OF TESTING 15
12.5 TESTING RESULTS 15

13 Results of the Evaluation **15**

14 Evaluator Comments, Observations and Recommendations 15

15 Glossary 16

15.1 ACRONYMS, ABBREVIATIONS AND INITIALIZATIONS.....16

16 References 17

Executive Summary

The Hercules® Automated Vulnerability Remediation (AVR), Version 2.2.0, from Citadel Security Software, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

The Hercules® AVR product is designed to operate on standard TCP/IP networks and can remediate vulnerabilities on Windows®, Solaris and Linux based clients. Hercules® AVR is a network security administration tool that is intended to be used in conjunction with advanced network vulnerability assessments. The purpose of the product is to enable the deliberate and controlled remote, automated vulnerability remediation of all classes of identified network vulnerabilities on large-scale, enterprise-level Windows® and Unix (Solaris/Linux) based networks. Hercules® AVR provides network security administrators with the ability to prioritize and remediate vulnerabilities using automated fixes that have been developed, tested and verified as being correct, and validated as being appropriate, by trusted and dedicated IT security professionals.

Fundamentally, the Hercules® AVR product provides enterprise administrators with the ability to manage a large-scale vulnerability remediation process in a manner that is both systematic and comprehensive. Today, many organizations employ an incomplete hybrid of manual and partially automated techniques that are often implemented in an ad-hoc manner. Hercules® AVR brings a defined and systematic maturity to these security-critical processes.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 27 February 2004, 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® AVR, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Hercules® AVR are advised to verify that their own environment is consistent with 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[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 1.0* (with applicable final

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

interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*.

CSE, as the CCS Certification Body, declares that the Hercules® AVR Version 2.2.0 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation is the Hercules® AVR, Version 2.2.0, from Citadel Security Software, Inc.

This report pertains to the TOE which is comprised of the following main components:

a. The Hercules® AVR Administrator Console;

b. One or more Hercules® AVR Servers;

c. One or more network devices with Hercules® AVR Clients installed on a supported Windows® operating system;

d. One or more network devices with Hercules® AVR Clients installed on a supported version of the Unix operating system; and

e. Applicable security functions of the underlying operating system.

2 TOE Description

The Hercules® AVR product is designed to operate on standard TCP/IP networks and can remediate vulnerabilities on Windows®, Solaris and Linux based clients.

The Hercules® AVR is a network security administration tool that is intended to be used in conjunction with advanced network vulnerability assessments. The purpose of the product is to enable the deliberate and controlled remote, automated vulnerability remediation (AVR) of all classes of identified network vulnerabilities on large-scale, enterprise-level Windows® and Unix (Solaris/Linux) based networks.

Hercules® AVR provides network security administrators with the ability to prioritize and remediate vulnerabilities using automated fixes that have been developed, tested and verified as being correct, and validated as being appropriate, by trusted and dedicated IT security professionals.

Hercules® AVR is designed to:

a. Aggregate vulnerability and remediation information from leading sources including SecurityFocus, BugTraq, CERTs and other Internet sources;

b. Import scan information from vulnerability scanners and combine this information to perform remediation from a single source;

c. Create profiles and remediation signatures that match scanner-independent vulnerability information and client machines with their corresponding remediations;

d. Allow an administrator to target network machines for automated remediation; and

e. Support Common Vulnerabilities and Exposures (CVE) compliance by displaying CVE identifiers and supporting searches based on them.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Hercules® AVR is identified in Section 5 of the ST.

4 Security Target

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

Title: Security Target Citadel Hercules® Automated Vulnerability Remediation Version 2.2.0

Version: v1.13
Date: 27 February 2004

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*, incorporating all final interpretations issued prior to 28 July 2003. The Hercules® AVR Version 2.2.0 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

6.1 Information Flow Control Security Functional Policy Hercules® AVR Server to Client [SERVER_SFP]

The only information that a Hercules® AVR Server will accept from any client machine is: (a) the identification of the client machine for authentication purposes when requesting a scheduled remediation, and (b) remediation status information during the course of a remediation session. All other information flow between the Hercules® AVR Server and a

Hercules® AVR Client will consist of remediation profiles or rollback instructions sent from the server to the client.

The operating environment for the TOE consists of a Hercules® AVR Administrator Console and one or more Hercules® AVR Servers connected in a network with a number of client machines. On a scheduled basis, the Hercules® AVR Server will automatically remediate vulnerabilities that are located on the client machines. In an environment where the client machines are assumed to contain vulnerabilities the possibility always exists that one or more of the client machines have been compromised and may act maliciously towards the TOE.

6.2 Information Flow Control Security Functional Policy Vulnerability Scanner Import [IMPORT_SFP]

If the vulnerability data is selected by an authorised TOE user and conforms to the expected format of data from one of the supported third party scanner products, then the TOE accepts that data as valid vulnerability information.

The TOE relies upon data generated by one or more third party vulnerability scanner products in order to identify the vulnerabilities that exist on client machines. These scanner products and their generated data fall outside the TOE. However, authorised TOE users may import data from one of the recognised scanner products into the TOE.

During the operation of the TOE the update of vulnerability remediation data must be performed on a regular basis. These updates are obtained from the trusted Hercules® AVR V-Flash server which falls outside the TOE boundary. The TOE uses Secure Sockets Layer (SSL) to ensure the integrity of the data downloaded from the V-Flash server.

7 Assumptions and Clarification of Scope

Consumers of the Hercules® AVR product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The Hercules® AVR product is designed for use by network administrators and it is assumed that they are appropriately trained and experienced. Further, it is assumed that the administrator has no malicious intentions and configures the product in accordance with its guidance documentation.

The Hercules® AVR product relies upon the underlying operating system (defined as part of the TOE) to provide some of the TOE security functions, as defined in its ST. It is assumed that the operating systems underlying the Hercules® AVR product are configured in

accordance with the Hercules® AVR Security Configuration Guide, and therefore can be trusted to function correctly.

7.2 Environmental Assumptions

In an environment where the Hercules® AVR client software is installed remotely on Windows® clients using the Hercules® AVR Client Management Services (CMS), the server and clients are assumed to reside on a protected network.

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

7.3 Clarification of Scope

This section lists and describes threats that consumers might reasonably believe to be countered by the TOE that, however, are actually not countered by the evaluated security functions of the described TOE.

The product will not prevent a user from carelessly configuring or using the Hercules® AVR such that network protection is compromised.

8 Architectural Information

The major components of the TOE consist of:

a. The Hercules® AVR Administrator Console provides the Human Machine Interface (HMI) for the product. It uses SSL-based communications with the Hercules® AVR Server(s), and has the ability to interact with Windows® user accounts, domain privileges and NT File System (NTFS) privileges. It authenticates (using Windows® integrated authentication) to Internet Information Server on the Hercules® AVR server. The Hercules® AVR Administrator Console is designed to be installed and used on a trusted and appropriately configured and controlled Windows® machine that is used for network administration. Users of the Hercules® AVR Administrator Console require full administrative privileges on the machine running the console as well as the Hercules® AVR Server and all client machines. The Hercules® AVR Administrator Console provides the HMI for the product and includes the display and input devices through which the user interacts with the Hercules® AVR application.

b. The Hercules® AVR Server is a Windows® service that communicates with the Hercules® AVR Client to distribute remediation profiles and gather remediation progress data. Multiple Hercules® AVR Servers may be deployed within a network and administered from a single Hercules® AVR Administrator Console. The Hercules® AVR Server is designed to be installed and used on a trusted and appropriately configured and controlled Windows® server.

c. The Hercules® AVR Windows® Clients are services that perform remediation activities on client machines. The clients establish Hyper Text Transfer Protocol , Secure (HTTPS)/SSL-based communication with the Hercules® AVR Server.

d. The Hercules® AVR Unix Clients provide functionality which is equivalent to Windows® client capabilities. Unix clients require a root account to install, configure, and execute Unix daemons, use of Unix file system access control and the use of Secure Shell (ssh) for installation.

The Hercules® AVR Administrator Console provides the product's HMI. It uses SSL-based communications with the Hercules® AVR Server(s), and has the ability to interact with Windows® user accounts, domain privileges and NT File System (NTFS) privileges. It authenticates (using Windows® integrated authentication) to Internet Information Server on the Hercules® AVR Server. The Hercules® AVR Server is a Windows® 2000/2003 service that communicates with the Hercules® AVR Client to distribute remediation profiles and gather remediation progress data. Multiple Hercules® AVR Servers may be deployed within a network and administered from a single Hercules® AVR Administrator Console. The Hercules® AVR Windows® Clients are NT/2000/XP/2003 services that perform remediation activities on client machines. The Hercules® AVR Unix Clients provide functionality equivalent to its Windows® clients.

9 Evaluated Configuration

The evaluated configuration of the Hercules® AVR Version 2.2.0 product (build 1792 with software update V-Flash Version 202000501, dated 2 Feb 2004) is described in detail in Hercules Security Configuration Guide, Hercules v2.2.0, February 2004, Document No. 205-01-0011, Document v2.1.

The Hercules® Security Configuration Guide provides procedures for securing the initial installation of Hercules® AVR Server v2.2.0, and defines how to configure Hercules® AVR to comply with Common Criteria EAL 3 requirements established in its ST.

The evaluated configuration of the Hercules® AVR Version 2.2.0 product (build 1792 with software update V-flash Version 202000501, dated 2 Feb 2004) consists of:

a. The Hercules® AVR Administrator Console executing on an Intel® Pentium based PC running Windows® 2000 Server with all service packs, Windows® 2000 Advanced Server with all service packs, Windows® XP Professional with all service packs, Windows® 2003 Standard Edition or Windows® 2003 Enterprise Edition as the operating system. Internet Explorer 5.5 or above is also required. The minimum hardware requirements for the Hercules® AVR Administrator Console are specified in the Citadel Hercules® AVR Automated Vulnerability Remediation Installation Guide. The required setup of the Hercules® AVR Administrator Console is described in the Hercules® AVR Security Configuration Guide.

b. One or more Hercules® AVR Server(s) executing on an Intel®Pentium based PC running Windows® 2000 Server with Service Pack 4, Windows® 2000 Advanced Server with Service Pack 4, Windows® 2003 Standard Edition or Windows® 2003 Enterprise Edition as the operating system. For the Windows® 2000 server family (Internet Information Server) IIS 5.0 is also required. For the Windows® Server 2003 family IIS 6.0 is also required. Internet Explorer 6.0 with service pack 1 is required for all installations. The minimum hardware requirements for a Hercules® AVR Server are specified in the Citadel Hercules® AVR Automated Vulnerability Remediation Installation Guide. The required setup of a Hercules® AVR Server is described in the Hercules® AVR Security Configuration Guide.

c. One or more network devices with Hercules® AVR Client Version 2.2.0 installed on a supported Windows® operating system. The supported versions of the Windows® operating system 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 SP, Windows® Server 2003 Standard 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. The minimum system requirements for Windows® Clients are specified in the Citadel Hercules® AVR Automated Vulnerability Remediation Installation Guide.

d. One or more network devices with Hercules® AVR Client Version 2.2.0 installed on a supported version of the UNIX operating system. The supported versions of the UNIX operating system are Solaris (SPARC) 2.6, 7, 8, 9 and Red Hat (Intel) 6.0, 6.1, 6.2, 7.0, 7.1, 7.2, 7.3, 8, 9. The minimum system requirements for UNIX Clients are specified in the Citadel Hercules® AVR Automated Vulnerability Remediation Installation Guide.

10 Documentation

The Citadel documents provided to the consumer – identified by their document number, version/issue number, and date – are as follows:

a. 204-01-0004 InstallGuide.pdf - Hercules Installation Guide, January 2004.

b. 205-01-0005 UserGuide.pdf – Hercules User Guide, January 2004.

c. 205-01-0006 HercRemedyGuide.pdf – Hercules Custom Remedy Guide, January 2004.

d. 205-01-0007 VulGuide.pdf – Hercules Vulnerability Assessment and Remediation Guide, January 2004.

e. 204-01-0008 IEAK.pdf – Creating Network Install Package for Microsoft Internet Explorer 6.0, January 2004.

f. 205-01-0009 Norton Restore.pdf – How to set Hercules to Manually Restore Norton/Symantec Antivirus Services Back to an Active Status, January 2004.

g. 204-01-0010 Office Installation Pack.pdf – Creating Network Administrative Installation Package to Apply Office Service Packs Using Hercules Remediation, January 2004.

h. 205-01-0011 SecurityGuide.pdf – Hercules Security Configuration Guide, v2.1, February 2004.

11 Evaluation Analysis Activities

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

Configuration management: An analysis of the Hercules® AVR development environment and associated documentation was performed. The evaluators found that the Hercules® AVR 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® AVR 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® AVR 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® AVR 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® AVR design and implementation.

Vulnerability assessment: The Hercules® AVR ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis. In addition, the evaluators performed an independent vulnerability and SOF analysis and developed tests that focused on potential vulnerabilities in the Hercules® AVR. Details are provided in section 12.3.

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

12 ITS Product Testing

Testing (coverage, depth, functional tests, independent testing): The evaluators examined the developer's testing activities and verified that the developer met their testing responsibilities.

12.1 Assessing Developer Tests

The evaluators verified that the developer met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Technical Report (ETR).

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 high-level 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.

A suitably configured TOE was evaluated in a controlled networked environment to confirm that TOE functionality operates as specified, and that the product can perform remediation on a representative set of well-known vulnerabilities from each of the vulnerability classes claimed by the developer. TOE functionality was evaluated in a real-world environment, using a representative set of network systems configured with known vulnerabilities. The Independent Functional Testing focused on:

a. Security of TOE after installation, generation and startup. The evaluators used the automated installation and set-up program compatible with the TOE operating system.

The installation process includes sufficient instructions to clearly document the installation process. The installation, generation and startup (IGS) results in the secure installation and start-up of the TOE. The evaluators repeated all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation and that the guidance facilitates the prevention and detection of insecure states as required by AVA_MSU.1. The installation, generation and startup of Hercules® AVR results in a configuration of the TOE that is in accordance with the TOE assurance measures M.SETUP, M.DOCS and M.DELIVER as defined in the Hercules® AVR ST.

b. Importing of Scanner and Remediation (User) Data. The evaluators verified the information flow control security functional policy [IMPORT_SFP] governing the import of vulnerability scan information and vulnerability remediation data from trusted external sources. The evaluators verified that the TOE has the capability of: (1) importing vulnerability scanner information from third party vulnerability scanners; (2) displaying imported scanner information; and (3) importing specific remediation information for reported vulnerabilities. If the vulnerability data is selected by an authorised TOE user and conforms to the expected format of data from one of the supported third party scanner products, then the TOE accepts that data as valid vulnerability information.

c. Approving vulnerabilities for remediation. The evaluators verified that the TOE allows authorized users complete control of the vulnerability and remediation data for all client systems, providing the user with: (1) an interface from which it is possible to manage the vulnerability scanner information and the vulnerability remediation information; (2) the capability for a suitably authorized user to manage remediation profiles; (3) the capability of displaying via a graphical user interface, the list of vulnerabilities that will be remediated by the Hercules® AVR Server for a client machine or a group of client machines; and (4) the capability to enable each device to allow each device to be remediated by its remediation profile. The evaluators verified that the management of vulnerability scanner information and the vulnerability remediation information was in accordance with the TOE security functions F.MANAGEDATA and F.MANAGEPROF as defined in the Hercules® AVR ST.

d. Integrity of VFlash service communications. The evaluators verified that all communication between a Hercules® AVR Remediation Server and the Citadel V-Flash server is via HTTPS. During the operation of the TOE the update of vulnerability remediation data must be obtained from the trusted Hercules® AVR VFlash server which falls outside the TOE boundary. The evaluators verified the integrity of data downloaded from the VFlash server in accordance with the TOE security functions F.ENCRYPT as defined in the Hercules® AVR ST.

e. Set-up and functioning of communications between Hercules® Administrative Console and Server. The evaluators verified that the Hercules® server supports the

use of certificates with HTTPS-based network communication. The Hercules® AVR Administrator Console has the capability to identify and authenticate each Hercules® AVR Remediation Server through the use of a certificate installed on the server. The Hercules® AVR Server has the ability to authenticate to the Windows Domain Controller using a Domain Administrator account with an internally generated, random password. The evaluators verified the functioning and performance of Hercules® AVR in accordance with the TOE security functions F.ENCRYPT and F.IAREMSVR as defined in the Hercules® AVR ST.

f. Confirm Interface between Hercules® Administrative Console and Server. The evaluators verified that the TOE uses SSL to secure data transfers between the Administrator Console and the Remediation Server(s) in accordance with the TOE security function F.ENCRYPT and F.IAREMSVR as defined in the Hercules® AVR ST.

g. Set-up and functioning of communications between Hercules® Server and Clients. With respect to supporting basic internal user data transfer protection, the evaluators verified that each Hercules® AVR Remediation Server has the capability to identify and authenticate each client machine for which it will issue a remediation profile. The client machines can be configured for HTTPS authentication with the Hercules® AVR server using a server certificate. In the evaluated configuration, the clients machines are configured with a client certificate for mutual authentication with the Hercules® AVR server. The evaluators confirmed that unauthorized Hercules client access to server is prevented by Windows and Unix client certificates in accordance with the TOE security function F.ENCRYPT, F.IACLIENT as defined in the Hercules® AVR ST.

h. Protection of internal transfer of remediation information (user data). The evaluators verified that the TOE uses SSL to secure data transfers between the server and clients. The evaluators verified the information flow control security functional policy governing sever-to-client communications [SERVER_SFP] and that the only information that a Hercules® AVR Server will accept from any client machine is: (a) the identification of the client machine for authentication purposes when requesting a scheduled remediation, and (b) remediation status information during the course of a remediation session, in accordance with the TOE security function F.ENCRYPT and F.IACLIENT as defined in the Hercules® AVR ST.

i. Usability of instructions for System hardening with IIS Lockdown tool. The evaluators confirmed that the TOE can be configured and used securely using only the supplied guidance documentation and that the guidance facilitates the prevention and detection of insecure states. The evaluators verified that the Hercules® Security Configuration Guide provides procedures to secure the TOE, after the initial installation and configuration of the product. The IGS and hardening of Hercules® AVR results in a secure installation and operational configuration of the TOE in

accordance with the TOE assurance measures M.SETUP, M.DOCS and M.DELIVER as defined in the Hercules® AVR ST.

j. Confirmation of audit capabilities. The evaluators verified that the Hercules® Security Configuration Guide provided procedures to configure additional Windows® audit settings, after the initial installation and configuration of the product, and that audit capabilities were in accordance with stated security functions in the ST. These tests confirmed that the Hercules® AVR Server is capable of generating audit events associated with the Windows Event Viewer application, security and system categories. As well, it was confirmed that the Hercules Event log was capable of logging Client Management Service, Patch Download Service and VFlash Service events in addition to the audit capabilities of the underlying operating system. The evaluators verified the functioning and performance of Hercules® AVR in accordance with the TOE security function F.AUDIT as defined in the Hercules® AVR ST.

12.3 Independent Penetration Testing

During this evaluation, the evaluator developed independent penetration tests based on an analysis of the developer's vulnerability analysis.

The penetration tests focused on:

a. Attempting to penetrate and read network communications between system components. Attempting to penetrate and read network communications between system components. The evaluators verified that network traffic was encrypted with SSL and verified that (1) the TOE uses SSL to secure data transfers between the Administrator Console and the Remediation Server(s), (2) the TOE uses SSL (for Windows® clients) and OpenSSH (for Unix clients) to secure data transfers between a Remediation Server and client systems. These functions prevent the unauthorized disclosure and/or modification of TSF data by protecting against the threat that a network attacker may intercept and monitor communications and use the information gained to compromise the TOE. Also, compromised VFlash updates are countered by HTTPS connection to Citadel VFlash Server. The TOE has the capability of encrypting data which is transferred between the physically separate elements of the TOE. The user can configure the Hercules® AVR Administrator Console to use HTTPS communication to the Hercules® AVR Remediation Server. The evaluators verified that eavesdropping on Hercules server network communication is countered by the ability to configure HTTPS-based communication amongst components of the TOE in accordance with the TOE security function F.ENCRYPT, F.IACLIENT and F.IAREMSVR as defined in the Hercules® AVR ST.

b. Scan Hercules® Server for obvious and publicly known vulnerabilities. The evaluators verified that the Hercules® Security Configuration Guide provides procedures to secure the TOE, after the initial installation and configuration of the product. The evaluators specifically verified that 1) only the Hercules virtual web server service is available using HTTPS; and 2) determined that the IIS server is more secure after hardening by performing a scan using a 3rd party vulnerability scanner. There was a noticeable improvement with fewer vulnerabilities for IIS after hardening than before. The IGS and hardening of Hercules® AVR results in a secure installation and operational configuration of the TOE in accordance with the TOE assurance measures M.SETUP, M.DOCS and M.DELIVER as defined in the Hercules® AVR ST.

c. Testing the I&A and Access Control Lists (ACLs) for Hercules® files and directories. The Hercules® AVR keeps unauthorised users from accessing data. The Hercules® AVR depends on Windows domain authentication and Windows Integrated Authentication by default and requires Administrative account permissions of the user. SSH-based authentication is used for Unix client management actions. The evaluators verified that the Hercules® Server application restricts access to only authorised administrator accounts and that a user with local admin privileges to their PC can not elevate rights and access the server. Having implemented the configuration settings described in the Hercules Security Configuration Guide (i.e., restrict user and group access to Hercules Server, restrict access to the Hercules working directory, and restrict access to the Hercules MS SQL database), the evaluators attempted but were unable to gain access the Hercules server using a rogue account and installation of the Administrative Console. The TOE protects Hercules® AVR file replacement by means of Windows Integrated Security and NTFS file system access control, and by limiting write access to Citadel directory to only Administrators. The evaluators verified that spoofed Hercules administrator actions are by countered by Windows Integrated Authentication via IIS configured by default.

d. Password capturing and cracking of internal TOE communication sessions. The evaluators performed a capture of the domain administrative account password used by the Hercules® AVR Server when authenticating to the Windows domain. A brute-force and dictionary attack was unsuccessful in obtaining this password, thus providing assurance in the SOF claim. The password was difficult enough to withstand a dictionary and brute force attack of moderate force. The evaluators verified that compromise of the HERC_CMS domain account password is prevented by the use of passwords meeting NSA requirements countering the threat of attacker cracking the domain account password to obtain credentials and higher privileges through privilege escalation.

e. Denial of Service (DOS) attacks against IIS. A network attacker may attempt to gain control of the Hercules® AVR Remediation Server. A denial of service attack was launched at the IIS service that provides the main interface to the Hercules® AVR

Server. The evaluators verified that the service was able to withstand the attack and still provide its interface to the Administrative Console, providing proof of the resiliency of the TSFI.

12.4 Conduct of Testing

The Hercules® AVR was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place at the Citadel Security Software, Inc.facility in Dallas Texas, and the ITSET facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. 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® AVR behaves as specified in its ST and functional specification.

The penetration testing resulted a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the Hercules® AVR in its intended operating environment.

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® AVR, Version 2.2.0 includes comprehensive Installation, User and Security Configuration Guides.

The Hercules® AVR, Version 2.2.0 is straightforward to configure, use and integrate into a corporate network.

The Hercules® AVR, Version 2.2.0 graphical user interface provided by the Hercules® AVR Administrator Console is intuitive and easy to use.

Citadel Security Software, Inc. Quality Assurance (QA) provides the requisite controls for managing all QA testing.

15 Glossary

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

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
ACL	Access Control List
AVR	Automated Vulnerability Remediation
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CMS	Client Management Services
CR	Certification Report
CSE	Communications Security Establishment
CVE	Common Vulnerabilities and Exposures
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMI	Human Machine Interface
IIS	Internet Information Server
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NTFS	New Technology (Microsoft Windows®) File System
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation

16 References

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

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Security Target, Citadel Hercules® Automated Vulnerability Remediation, Version 2.2.0, Document No. 1451-011-D001, Version 1.13, 27 February 2004.

e) Evaluation Technical Report (ETR), Citadel Hercules® Automated Vulnerability Remediation (AVR) Version 2.2.0, EAL 3 Evaluation, Common Criteria Evaluation Number, 383-4-18, Document No. 1451-000-D002, Version 0.5, 24 February 2004.