Maintenance Report

Citadel Hercules® Automated Vulnerability Remediation (AVR)

Version 3.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-2-MR
Version: 1.0
Date: 19 August 2004
Pagination: 1 to 3

1 Introduction

On 22 July 2004, Electronic Warfare Associates-Canada (EWA-Canada) submitted an Impact Analysis Report to the CCS Certification Body on behalf of Citadel Security Software Incorporated, the developer of the Citadel Hercules® Automated Vulnerability Remediation product. The Impact Analysis Report is intended to satisfy requirements outlined in version 1.0 of the Common Criteria document CCIMB-2004-02-009: Assurance Continuity: CCRA Requirements. In accordance with those requirements, the Impact Analysis Report describes the changes made to Citadel Hercules® Automated Vulnerability Remediation version 2.2.0 (the certified Target of Evaluation), the evidence updated as a result of the changes, and the security impact of the changes.

2 Description of changes

The following changes are implemented in version 3.0 of Citadel Hercules® Automated Vulnerability Remediation.

2.1 Feature changes

The following features were added for version 3.0. For each of these features, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted to ensure that the assurance in the original certified Target of Evaluation (TOE) was maintained.

- **Hercules® Channel Server and Hercules® File Download Server**. These two components can now be optionally broken out from the previous Hercules® Server to provide for a distributed architecture configuration that can improve data flow and optimize bandwidth across dispersed networks.

- **Graphical User Interface**. The new interface for the Hercules® Administrator is now *action oriented* (where actions or tasks are selected and applied to devices), rather than *device oriented* (where devices are selected, then actions or tasks are selected, then the actions or tasks are assigned to the devices). In addition, context-sensitive help is now provided on-line.

- **Remediation Capabilities**. A remediation policy can now be defined and enforced where remedies are applied to devices regardless of vulnerabilities detected by third party scanners.

- **ConnectGuard.** This feature can be used to prevent clients that have been disconnected from the network from gaining network access until the remediation policy has been applied.

- **Pre-defined roles**. There are now six pre-defined user roles available, with each role able to perform particular tasks on particular devices.

- **Device Discovery**. An Import Wizard function discovers and displays the Microsoft® Windows NT® Domain structure and the Microsoft® Active Directory® structure, allowing selection of devices for import. A comma-delimited flat file import containing devices and their attributes is now supported.

- **Scripting**. A new Scripting Methods Reference allows the running of custom scripts from remedies.

2.2 Bug fixes

There were a number of minor code changes as a result of defects detected and resolved through the QA/test process. For each of these changes, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted for each code change, to ensure that the assurance in the original certified TOE was maintained.

2.3 Development environment changes

Other compatible tools for source code control and test management are now used. The changes are limited in scope and do not affect the manner in which the configuration management system tracks the evolution of the product, or the way in which the TOE is developed and tested.

3 Affected developer evidence

Modifications to the TOE and the development environment necessitated changes to a subset of the developer evidence that was previously submitted for the certified TOE. The set of affected developer evidence was correctly identified, and revised versions of all affected developer evidence were submitted.

4 Conclusions

The changes comprised feature changes, bug fixes, and development environment changes. None of these changes required any modification to the security functional requirements in the ST, nor were there any changes to the existing security assurance requirements. Thorough functional and regression testing of Citadel Hercules® Automated Vulnerability Remediation Version 3.0 led to the conclusion that security assurance was maintained. Consideration of each of the changes leads to the conclusion that the changes are classified as minor, and that maintenance is the correct path to continuity of assurance.

5 References

Assurance Continuity: CCRA Requirements, CCIMB-2004-02-009, version 1.0, February 2004.

Technical Oversight for Assurance Continuity of a certified TOE, version 1.0, 18 June 2004.

Certification Report for EAL3 Evaluation of the Citadel Hercules AVR Version 2.2.0 , version 1.1, 1 March 2004.