Certification Report

EAL 2+ Evaluation of Harris Corporation

STAT Guardian™ Vulnerability Management Suite (VMS):
STAT® Scanner 6.4.0
STAT® Patch and Remediation 6.4.0
STAT® Report Center 6.4.0
STAT® Command Center 6.4.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-45-CR
Version: 1.0
Date: 23 May 2006
Pagination: i to v, 1 to 11

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 May 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 at:
http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html

This certification report makes reference to the following trademarks or registered trademarks:

- Guardian and STAT are either trademarks or registered trademarks of Harris Corporation 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.;
- PatchLink Update is a trademark of Patchlink Corporation in the United States and/or other countries;
- 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; and
- UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

TABLE OF CONTENTS

Executive Summary

The STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0, from Harris Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation.

The STAT Guardian™ VMS is a suite of network management tools that provides IT professionals with the capability to perform network vulnerability assessments, apply latest vendor patches, and generate enterprise reports from a single user interface.

The STAT Guardian™ VMS supports the following range of target operating systems: Microsoft® Windows® NT/2000/XP/2003, Sun™ Solaris™, RedHat® Linux®, Fedora™ Linux, Mandriva Linux™, SuSE Linux®, HP-UX®, Apple® Mac OS X®, BSD-Unix variants, and network devices and printers (i.e., Cisco IOS™, Cisco CATOS™, Cisco VPN™, Cisco PIX™, Juniper JUNOS™, Foundry® switches and routers, and HP® printers).

Vulnerability cross-referencing is supported for the following advisory lists: United States Computer Emergency Readiness Team (US-CERT), Common Vulnerabilities and Exposures (CVE), Computer Incident Advisory Capability (CIAC), SANS, National Institute of Standards and Technology (NIST), and US Department of Defense (DoD), US Army, Navy, and Air Force Information Assurance Vulnerability Management (IAVM).

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 12 May 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 STAT Guardian™ VMS, 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 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 indicate that it meets the EAL 2+ 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

[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.

the *Common Criteria for Information Technology Security Evaluation, version 2.2*. The following augmentations are claimed:

- ACM_CAP.4 - Generation support and acceptance procedures;
- ACM_SCP.1 – TOE configuration management coverage;
- ALC_DVS.1 – Identification of security measures;
- ALC_FLR.3 – Systematic flaw remediation;
- ALC_LCD.1 – Developer defined life-cycle model; and
- AVA_MSU.1 – Examination of guidance.

The Communications Security Establishment, as the CCS Certification Body, declares that the STAT Guardian™ VMS 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) 2+ evaluation is the STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0, from Harris Corporation (hereafter referred to as the STAT Guardian™ VMS).

2 TOE Description

The STAT Guardian™ VMS is a suite of network management tools that provides the capability to perform network vulnerability assessments, apply vendor patches, and generate enterprise reports from a single user interface. The STAT Guardian™ VMS provides the following functionality:

- The STAT® Scanner performs network vulnerability assessments and supports a wide variety of operating systems, enterprise applications, and software and firmware configurations.
- The STAT® Patch and Remediation integrates the vulnerability assessment and enterprise reporting capabilities of STAT® Scanner with PatchLink Update™ Server to provide agent-based vulnerability scanning and remediation.
- The STAT® Report Center provides users the ability to consolidate vulnerability scan and remediation data from multiple STAT® Scanner installations.
- The STAT® Command Center combines the enterprise data collection capabilities of STAT® Report Center with the ability to configure and schedule distributed vulnerability scanning and remediation.

3 Evaluated Security Functionality

Security functionality detail 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: STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0 Security Target
Version: Revision No. 1.13
Date: 20 April 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, Revision 326, December 2004.* The STAT Guardian™ VMS 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 2 augmented, containing all security assurance requirements from EAL 2, as well as the following: ACM_CAP.4, ACM_SCP.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, AVA_MSU.1.

6 Security Policy

The STAT Guardian™ VMS 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. STAT Guardian™ VMS security policy detail can be found in Section 2.2.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the STAT Guardian™ VMS 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 STAT Guardian™ VMS.

7.1 Secure Usage Assumptions

Personnel authorized to install, configure, and operate the STAT Guardian™ VMS possess appropriate training, are not willfully negligent or hostile, and will adhere to the procedures for secure usage of the product.

Organizations operating the STAT Guardian™ VMS have backup and recovery procedures allowing the STAT Guardian™ VMS to be recovered to a secure configuration after a hardware failure.

7.2 Environmental Assumptions

The STAT Guardian™ VMS resides in a secure networked environment.

Microsoft Windows Server 2003, the host operating system upon which the STAT Guardian™ VMS resides, has been installed, configured and security-hardened in

accordance with the Microsoft Windows Server 2003 Service Pack 1 Installation and Deployment Guide.

7.3 Clarification of Scope

The STAT Guardian™ VMS provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. It is designed to protect its user community against inadvertent or casual attempts to breach system security, by attackers possessing a low attack potential. It is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

Figure 2.2.1 of the ST shows the STAT Guardian™ VMS component configuration.

The STAT Guardian™ VMS Graphical User Interface (GUI) is the user's access point to product functionality. The user uses the STAT Guardian™ VMS GUI to connect to either a STAT® Scanner engine or a STAT® Report Center engine. Based on the type of engine, the GUI will automatically configure itself to present the appropriate interface.

The STAT® Scanner Engine runs as a registered Windows service under a local administrator account. The STAT® Scanner Engine is a Simple Object Access Protocol (SOAP) service that exposes a user interface to discover targets, assess vulnerabilities, and generate custom reports from collected data. A STAT® Patch and Remediation license key unlocks additional functionality in the Scanner Engine component allowing it to interface with a PatchLink Update™ Server for agent-based scanning and remediation.

The STAT® Report Center engine runs as a registered Windows service under the local administrative account. The Report Center interface allows users to manage, aggregate, and report enterprise vulnerability and remediation data. A STAT® Command Center provides Report Center users with the additional capability to perform distributed scanning and remediation. A STAT® Command Center license augments the Report Center interface with functions for configuring and scheduling vulnerability scanning and remediation on multiple remote Scanner systems.

The STAT Guardian™ VMS Database serves as a repository for both local and remotely collected scan and agent data as well as security attributes. The default installation of the STAT Guardian™ VMS Database uses Microsoft SQL Server Desktop Engine (MSDE).

9 Evaluated Configuration

The evaluated configuration for the STAT Guardian™ VMS comprises:

- STAT® Scanner 6.4.0 with STAT® Patch and Remediation 6.4.0 running on Microsoft Windows 2003 Server; and
- STAT® Report Center 6.4.0 with STAT® Command Center 6.4.0 running on Microsoft Windows 2003 Server.

The configuration is described in detail in the STAT Guardian™ Vulnerability Management Suite (VMS) Installation and Security Guide.

10 Documentation

The documents provided to the consumer are:

- STAT Guardian™ Vulnerability Management Suite (VMS) Installation and Security Guide, Document No. 8014725, Revision No. 2.2, 11-Apr-06;
- Release Notes for STAT Guardian™ Vulnerability Management Suite (VMS) Version 6.4, 21-Nov-05; and
- STAT Guardian™ VMS Users Guide, 15-Feb-06.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the STAT Guardian™ VMS, including the following areas:

Configuration management: An analysis of the STAT Guardian™ VMS development environment and associated documentation was performed. The evaluators found that the STAT Guardian™ VMS 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 STAT Guardian™ VMS 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 STAT Guardian™ VMS 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 STAT Guardian™ VMS 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 STAT Guardian™ VMS design and implementation. The documented flaw remediation process was carefully reviewed, demonstrating that adequate procedures are in place to track and correct security flaws, and distribute the flaw information and corrections. In addition, the evaluators verified that the development team has a detailed, mature and well-practised life-cycle model for the STAT Guardian™ VMS development and maintenance.

Vulnerability assessment: The STAT Guardian™ VMS ST strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the STAT Guardian™ VMS 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. Limited 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 at EAL2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the ETR.

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

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.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The tests focused on:

- Audit;
- User data protection;
- Identification and authentication;
- Security roles; and
- Protection of the security functions.

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 STAT Guardian™ VMS in the anticipated operating environment.

12.4 Conduct of Testing

The STAT Guardian™ VMS 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 STAT Guardian™ VMS behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2+** 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 STAT Guardian™ VMS includes a comprehensive Installation and Security Guide and Users Guide.

The STAT Guardian™ VMS is straightforward to configure, use and integrate into a corporate network.

Harris Corporation Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

Glossary

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

14.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIAC	Computer Incident Advisory Capability
CM	Configuration Management
CSE	Communications Security Establishment
CVE	Common Vulnerabilities and Exposures
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IAVM	Information Assurance Vulnerability Management
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MSDE	Microsoft SQL Server Desktop Engine
NIST	National Institute of Standards and Technology
PALCAN	Program for the Accreditation of Laboratories Canada
POSIX	Portable Operating System Interface
QA	Quality Assurance
SANS	SysAdmin, Audit, Network, Security
SOAP	Simple Object Access Protocol
STAT	Security Threat Avoidance Technology
ST	Security Target
TOE	Target of Evaluation
US-CERT	United States Computer Emergency Readiness Team
VMS	Vulnerability Management Suite

15 References

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

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

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. STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4 Security Target, Document No. 8014721, Revision No. 1.13, 20 April 2006.

e. Evaluation Technical Report (ETR) STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-45, Document No. 1515-000-D002, Version 0.3, 26 April 2006.