Certification Report

EAL 2+ Evaluation

Of

Harris Corporation

STAT® Scanner Professional

Version 5.08

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-15
Version:	1.0
Date:	9 April 2003
Pagination:	i to iv, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 1.0, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the Communications Security Establishment (CSE) or by any other organisation that recognises or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organisation that recognises or gives effect to this report, and 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. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, managed by the Communications Security Establishment.

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the CCS Certification Body for approval to perform Common Criteria evaluations. A significant requirement for such approval is accreditation to the requirements of the *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, Limited, located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that a product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines and scopes 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 (evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 9 April 2003, 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 Canadian 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: STAT, which is a registered trademark of Harris Corporation; Windows NT and Windows 95/98/Me/2000/XP, which are registered trademarks of Microsoft Corporation; Red Hat, which is a trademark of Red Hat, Inc.; Linux, which is a registered trademark of Linus Torvalds; Sun and Solaris, which are trademarks of Sun Microsystems, Inc.; and UNIX, which is a registered trademark of the Open Group.

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

STAT® Scanner Professional Version 5.08 from Harris Corporation is the target of evaluation for this EAL 2 augmented evaluation. It is most accurately described as an internal network vulnerability assessment tool. It supports the ability to statically monitor a set of IT resources in order to identify configurations that may be indicative of potential vulnerabilities in, or misuse of, those IT resources. This is accomplished by comparing the information collected with a database of known vulnerabilities. STAT® Scanner Professional helps keep network computer configurations up-to-date with current patches, security roll-ups, and service packs by assessing the IT resources and providing the administrator with the required information to update configurations. STAT® Scanner Professional supports a range of target operating systems: Windows® NT/95/98/Me/2000/XP, RedHat™ Linux 6.2 and later, Mandrake™ Linux 7.1 and later, and Sun™ Solaris 2.5.1 and later.

Electronic Warfare Associates-Canada (EWA-Canada) is the Common Criteria evaluation facility that conducted the evaluation. This evaluation was completed on 7 April 2003, 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 the intended environment for the STAT® Scanner Professional, 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 STAT® Scanner Professional are advised to verify that their own environment is consistent with the environment identified 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[1] for this product indicate that it meets the Evaluation Assurance Level 2 augmented requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1, August 1999*. The following augmentations are claimed:

a. ACM_CAP.4 - Generation support and acceptance procedures;

b. ACM_SCP.1 – TOE configuration management coverage;

c. ALC_DVS.1 – Identification of security measures;

d. ALC_FLR.3 – Systematic flaw remediation;

e. ALC_LCD.1 – Developer defined life-cycle model; and

f. AVA_MSU.1 – Examination of guidance.

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

STAT® Scanner Professional Version 5.08 conforms with the *IDS Scanner Protection Profile, Version 1.1, December 10, 2001*.

The Communications Security Establishment, as the CCS Certification Body, declares that the STAT® Scanner Professional Version 5.08 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the Certified Products List.

1 Identification of Target of Evaluation

The Target Of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is the STAT® Scanner Professional Version 5.08 (hereafter referred to as the STAT® Scanner).

The TOE includes Windows® 2000 security functions. The evaluation approach included the re-use of Windows® 2000 evaluation results. Windows® 2000 was certified within the US Common Criteria Evaluation and Validation Scheme (CCEVS) to EAL 4, augmented by ALC_FLR.3 (Systematic Flaw Remediation). Reference is made to Common Criteria Certificate and Validation Report number *CCEVS-VR-02-0025 Version 2.0*, dated 25 October 2002.

2 Product Description

STAT® Scanner performs security vulnerability analysis of Windows® NT 3.51/4.0; Windows® 95/98/Me/2000/XP network services; Red Hat™ Linux® 6.2 and later; Mandrake™ Linux 7.1 and later; and Sun™ Solaris™ 2.5.1 and later.

STAT® Scanner collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion on an Information Technology (IT) System. The information collected is obtained from a variety of sources located on an IT System and is securely managed until it can be delivered to analysis functions.

STAT® Scanner can run on the following host operating systems: Microsoft Windows® 2000, Microsoft Windows® NT® 4.0 Service Pack 3 and later, and Microsoft Windows® XP. Prospective consumers should refer to section 9, of this certification report, for a complete description of the evaluated configuration, as the STAT® Scanner was not evaluated on all of the aforementioned operating systems.

Refer to the Security Target (ST), Figure 2-3, for a typical configuration for the STAT® Scanner host machine and its interactions when scanning remote target machines.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the STAT® Scanner is identified in Section 5.1 of the ST.

4 Security Target

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

STAT® Scanner Professional Version 5.08 Security Target
Common Criteria EAL 2 (augmented)
Harris Document 8008352 Revision C
Date: April 7, 2003

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*. The STAT® Scanner Version 5.08 is:

a) Common Criteria *Part 2 extended*, with security functional requirements based upon functional requirements in Common Criteria Part 2 and in the *IDS Scanner Protection Profile, Version 1.1, December 10, 2001*; and

b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c) Common Criteria EAL 2 compliant, augmented with:

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

STAT® Scanner Professional Version 5.08 conforms with the *IDS Scanner Protection Profile, Version 1.1, December 10, 2001.*

6 Security Policy

The STAT® Scanner security policies are described in this section.

6.1 Identification and Authentication

No access is granted, and thus no actions may be taken, until successful identification and authentication (I&A) has been completed. The only authorized user of the STAT® Scanner is that of a system or domain administrator.

6.2 Security Management (Access Control)

Only authorized administrators may modify the behaviour of the STAT® Scanner for sensor data collection and review. Only authorized administrators may modify or access scanner and audit data.

6.3 Auditing

STAT® Scanner protects the audit records by ensuring that only authorized personnel (system administrators) have access to the audit records. In addition, any attempt, whether authorized or not, to access, modify, or delete the audit record data, vulnerability database, or user credential information, will be logged and can only be reviewed by an authorized user. STAT® Scanner provides auditing of scanner functions such as start, stop, and abnormal termination of a scan. The audit records are protected from deletion, modification and system failures. Modifications to audit records are also recorded.

6.4 Protection of Security Functions and Data Integrity

STAT® Scanner provides:

a. a secure domain for each program execution and protects each program execution from interference and tampering;

b. separation mechanisms between domains; and

c. reliable non-decreasing time stamps for use with auditing events.

6.5 IDS (Scanner Data Collection and Presentation)

STAT® Scanner enforces the following IDS (Scanner data collection and presentation) security policy:

a. checking of static configuration information from the target IT system resources for possible vulnerabilities and offering advice on methods to mitigate risks identified for the categories of vulnerability;

b. providing a list of attributes associated with each vulnerability identified during an assessment, and also providing reference materials, advisories and articles related to the vulnerability if available, along with brief evidence of the vulnerability;

c. protecting Scanner data from unauthorized modification and loss;

d. protecting Scanner data from loss due to storage exhaustion and failure; and

e. preventing Scanner data collection/presentation actions, except those taken by an authorized user with special rights, and sending an alarm if the storage capacity has been reached.

7 Assumptions and Clarification of Scope

Consumers of this product should consider assumptions about TOE usage and environmental settings as requirements for the product's installation and operating environment. This will ensure the proper and secure operation and functionality of the TOE.

7.1 Secure Usage Assumptions

a. Only authorized administrators may access the TOE host and software.

b. Administrators are assumed to be trusted and competent to carry out their tasks when using the TOE. It is assumed that the authorized administrator(s) will follow and abide by the instructions provided by the TOE documentation with non-malicious intent.

c. A strong password policy is to be in place and enforced.

d. An account lockout policy is to be implemented. After a specific number of invalid attempts a user's account will lockout and require administrative intervention.

e. The Windows® NTFS file system must be in place to provide file-locking mechanisms for audit data while it is in use.

f. In order to obtain a more accurate assessment of vulnerabilities on a Windows® target, access to NetBIOS Admin share[2] access is desired. This access provides greater certainty and a more reliable method of vulnerability assessment through direct examination of files instead of relying solely on the registry, which can sometimes lead to false-positive identifications. With respect to the secure use of Admin share, it is assumed that the authorized administrator(s) will follow and abide by the instructions provided by the TOE documentation and properly configure the IT system (e.g., null session disabled and ports closed in accordance with the STAT® Scanner Installation and User's Guide).

7.2 Environmental assumptions

It is assumed that the TOE has access to all the IT system data it needs to perform its functions. The TOE depends on the correct functioning of the IT system (Domain Controller, Unix system security access components, Windows® 2000 system security access components, Network infrastructure and mapping).

[2] *Admin share should not be confused with the enabling of local folders to be shared with others on your network.*

The TOE is presumed to be located within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

Windows® 2000 provides the following TOE security functions: I&A, Security Management, Data Availability, Protection of Security Functions and most Audit capabilities.

8 Architectural Information

The TOE comprises the following functional components:

1. *Identification and Authentication (I&A)* - provided to users through the Windows® 2000 I&A mechanisms (Winlogon), which are user-id and password based;

2. *Graphical User Interface (GUI)* - the primary user interface provided when the application is launched is the graphical user interface. This interface allows most commands to be executed that are involved in the operation of the TOE. This executable is launched from the user menu or desktop icon link after product installation;

3. *Command Line Interface (CLI)* - a command line interpreter exists for use by batch processing programs or third party programs that invoke STAT® Scanner using a shell. Only a subset of the full set of TOE features is available using the CLI;

4. *Scanner Engine* - provides an application-programming interface (API) to the GUI or CLI, and is at the core of the TOE scanning abilities;

5. *Vulnerability Threads* - the threads, created by the main task, run a specific vulnerability assessment against a target machine;

6. *Report Viewer* - this is used to display reports;

7. *Target Discovery* - the function of target discovery is for network discovery of target machines and to determine and record their operating system; and

8. *Target Administration and Establishing User Credentials* - the user supplies credentials for remote target access.

9 Evaluated Configuration

The evaluated configuration comprises: the STAT® Scanner Professional Version 5.08, a Windows® 2000 platform with supporting devices including a Network Interface Card, and the user guidance documentation describing the correct configuration and operation of the

TOE. The correct configuration is described in detail in the *STAT® Scanner Professional Edition Installation and Users Guide, Version 5*.

10 Documentation

The STAT® Scanner comes with a copy of the installation and user manual, *STAT® Scanner Professional Edition Installation and Users Guide Version 5*. This manual provides a list of: administrative and system requirements; installation and security configuration guidance; user guidance; and customisation and troubleshooting sections.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the STAT® Scanner, including the following areas:

Configuration management: An analysis of the STAT® Scanner development environment and associated documentation was performed. The evaluators found that the STAT® Scanner configuration items were clearly marked, and had the ability to be modified and controlled. The developer's configuration management system was observed during a site visit and found to be mature and well-developed.

Secure delivery and operation: The evaluators examined the delivery documentation that describes the procedures used to maintain the integrity of STAT® Scanner during its generation from the development environment through to delivery to the customer. These procedures were found to be sufficient to maintain the integrity of STAT® Scanner. The evaluators tested the installation, generation and start-up procedures in the document "*STAT® Scanner Professional Edition Installation and User's Guide*" and determined that they were complete and in sufficient detail to result in a secure configuration.

There presently exists two delivery methods for STAT® Scanner. The most common method is the use of the Internet for download using a secure SSL (Version 3.0) session. An MD5 checksum is available so that customers may confirm that the downloaded file is identical to the original. The second method of delivering the product is on compact disk through commercial parcel post, and was observed by the evaluation team. Although this process is rarely used, it serves as a backup to the online delivery mechanism and is described in detail in the delivery documentation.

Design documentation: The evaluators analysed the STAT® Scanner functional specification and high-level design, and determined that they were internally consistent, completely and accurately instantiated all interfaces and security functions, and independently validated the correspondence mappings between the design documents were correct.

Guidance documentation: The evaluators examined the STAT® Scanner user and administrator guidance documentation and determined that the documentation sufficiently and unambiguously describes how to securely use and administer the product, and that it was consistent with all other documents supplied for evaluation.

Life-cycle support: Development security procedures were assessed during a site visit and were found to provide adequate confidentiality, integrity during the development of STAT® Scanner. 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® Scanner development and maintenance.

Vulnerability assessment: The evaluator examined the developer's STAT® Scanner vulnerability analysis, and supplemented the developer's analysis with their own independent vulnerability analysis, and development of potential penetration tests.

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

12 ITS Product Testing

Testing (coverage, functional tests, independent testing): The evaluators examined the developers' testing coverage. EWA-Canada verified that the developer has met their testing responsibilities through an examination of testing evidence, a review of the test results, and an on-site visit to Harris Corporation.

12.1 Testing Coverage

The evaluators verified that the developer had met their testing responsibilities through an examination of testing evidence, a review of the test results, and an on-site visit to Harris Corporation. The evaluator's follow-on approach to testing was to test a representative subset of the TOE security functions as defined in the ST and the functional specification.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of EWA-Canada test goals:

a. Test Goal No. 1 - Test Installation Procedures;

b. Test Goal No. 2 - Test I&A Mechanisms;

c. Test Goal No. 3 - Test Access Control Mechanisms;

d. Test Goal No. 4 - Tests Scanner Function;

e. Test Goal No. 5 - Test Audit Mechanisms; and

f. Test Goal No. 6 - Vulnerability Assessment Test Procedure.

12.2 Penetration Testing

Penetration/vulnerability tests were devised using the STAT® Scanner vulnerability analysis and associated misuse and strength of function analyses, the functional specification, the high-level design, the ST, and the installation and users guide. The tests focused on: protection of audit and STAT® Scanner data, specifically guarantee of data availability and prevention of data loss; protection of security functions; and protection against denial of service; and checks for vulnerabilities in supporting packages.

12.3 Conduct of Testing

The TOE was subjected to an extensive and comprehensive suite of formally documented independent functional and penetration tests during a three-month period. The testing took place at the ITSET Facility at Electronic Warfare Associates–Canada, Limited located in Ottawa, Ontario. The CCS certification body witnessed a portion of this independent testing

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are defined and documented in the Evaluation Technical Report (ETR)[3].

12.4 Testing Results

Upon examining the developer's analyses of test coverage and depth, the evaluators confirmed that all of the TOE security functions were tested and operating in accordance with the functional specification. The developer's tests and the independent functional tests yielded the expected results, giving assurance that the TOE behaves as specified in its ST and design documentation.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2+** level of assurance, including the augmentations identified in section 5 of this report. All evaluation activities resulted in a PASS verdict. These results are supported by evidence contained in the ETR.

[3] The Evaluation Technical Report is an internal document to the CCS that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review

14 Evaluator Comments, Observations and Recommendations

14.1 Evaluator comments

14.1.1 Documentation

The complete documentation for the STAT® Scanner consists of a comprehensive Installation and Users Guide and in-depth, context-sensitive online Help and Web functions.

14.1.2 Configuration

The STAT® Scanner is straightforward to configure, use and integrate into a corporate network.

14.1.3 Product reporting

The reporting capabilities of the STAT® Scanner are extensive and useful.

14.1.4 Ease of use

The STAT® Scanner graphical user interface is intuitive and easy to use.

15 Acronyms and Abbreviations

Acronym/Abbreviation	Description
API	Application Programming Interface
CB	Certification Body
CCEF	Common Criteria Evaluation Facility
CCEVS	Common Criteria Evaluation and Validation Scheme
CCS	Canadian Common Criteria Evaluation and - Certification Scheme
CLI	Command Line Interface
CM	Configuration Management
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication
IDS	Intrusion Detection System
IT	Information Technology
ITSET	IT Security Evaluation and Test
NTFS	NT File System
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
STAT	Security Threat Avoidance Technology
TOE	Target of Evaluation

16 References

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

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

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

3. Common Methodology for Information Technology Security Evaluation Supplement ALC_FLR Flaw Remediation, CEM-2001/0015R, Version 1.1, February 2002.

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

5. STAT® Scanner Professional Version 5.08 Security Target, Document 8008352, Revision C, April 7, 2003.

6. Evaluation Technical Report (ETR), Harris Corporation STAT® Scanner Professional Version 5.08, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-15, Document No. 1442-000-D002, Version 0.8, 8 April 2003.

7. Windows 2000 Security Target Version 2.0, dated 18 October 2002

8. National Information Assurance Partnership (NIAP) Common Criteria Certificate and Validation Report (Number CCEVS-VR-02-0025, Version 2.0, 25 October 2002) for Microsoft Corporation Windows 2000.