Certification Report

EAL 3+ Evaluation of Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V5.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-148-CR
Version: 1.0
Date: 22 May 2012
Pagination: i to iii, 1 to 9

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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. 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 Canada, 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 Communications Security Establishment Canada, 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 Canada.

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/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration 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 EWA-Canada located in Ottawa, Canada.

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 22 May 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks:

- Rapid7™ and Nexpose™ are trademarks of Rapid7 LLC.

TABLE OF CONTENTS

Executive Summary

Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V5.1 (hereafter referred to as Nexpose™), from Rapid7 LLC, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Nexpose™ is a vulnerability scanner and vulnerability management tool that supports policy compliance checking, web application scanning, and penetration testing. Nexpose™ scans a specified list or range of Internet Protocol (IP) addresses and collects information about the devices that it finds.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 May 2012 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 Nexpose™, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Nexpose™ evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

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

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V5.1 (hereafter referred to as Nexpose™), from Rapid7 LLC.

2 TOE Description

Nexpose™ is a software-only TOE comprising the Nexpose™ Security Console (NSC) and the Nexpose™ Scan Engine (NSE).

Nexpose™ is a vulnerability scanner and vulnerability management tool that supports policy compliance checking, web application scanning, and penetration testing. Nexpose™ scans a specified list or range of Internet Protocol (IP) addresses and collects information about the devices that it finds. Approved users can access the collected data the through a web interface and generate reports to perform analysis of monitored devices and events. The NSC is the central management tool for Nexpose™ and the NSE profiles a section, or sections, of network space specified in blocks of IP addresses.

A detailed description of the Nexpose™ architecture is found in Section 1.4.1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Nexpose™ is identified in Section 5 of the ST.

4 Security Target

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

Title: Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1 Security Target
Version: 1.7
Date: 11 May 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Nexpose™ 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 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

Nexpose™ implements a Data Access Security Policy which restricts access to vulnerability scan data and asset information to authorized users. Details of this security policy can be found in Section 5 of the ST.

In addition, Nexpose™ implements policies pertaining to security audit, identification and authentication, security management, and TOE access. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

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

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks;
- Those responsible for the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation; and
- Users of the TOE possess the necessary privileges to access information managed by the TOE.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The Secure Socket Layer (SSL) connection between the user's browser and the TOE, and the SSL-connection between the NSC and the NSE are secure;
- The components of the TOE are to be connected to the target network at all times;

- The TOE is installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product;
- The TOE hardware and software are delivered, installed, and setup in accordance with documented delivery and installation/setup procedures;
- The TOE is interoperable with the IT System that it monitors;
- The TOE hardware and software critical to security policy enforcement are assumed to be within controlled access facilities, preventing unauthorized physical access and modification by potentially hostile outsiders; and
- The update server and support site with which the TOE communicates are under the same management control and operated under the same security policy constraints as the TOE.

7.3 Clarification of Scope

Nexpose™ offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Nexpose™ is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Nexpose™ comprises the Nexpose™ Security Console version 5.1 and the Nexpose™ Scan Engine version 5.1 in the following configurations:

- Build 2220601069 running on Ubuntu 8.04 32-bit Standard and Cloud Edition;
- Build 839270008 running on Ubuntu 8.04 64-bit and Red Hat Enterprise Linux 5.4 64-bit Standard and Cloud Edition;
- Build 1220461598 running on Windows Server 2003 SP2 32-bit and Windows XP SP3 32-bit Standard and Cloud Edition; and
- Build 3456844061 running on Windows Server 2003 SP2 64-bit Standard and Cloud Edition.

The publication entitled *Rapid7 Nexpose™ Common Criteria Configuration Guide version 1.1* describes the procedures necessary to install and operate Nexpose™ in its evaluated configuration.

9 Documentation

The Rapid7 LLC documents provided to the consumer are as follows:

a. Nexpose 5.1 Software Installation and Quick-start Guide, January 2012;

b. Nexpose 5.1 Administrator's Guide, January 2012;

c. Nexpose 5.1 User's Guide, January 2012; and

d. Rapid7 Nexpose™ Common Criteria Configuration Guide version 1.1.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Nexpose™, including the following areas:

Development: The evaluators analyzed the Nexpose™ functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Nexpose™ security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Nexpose™ preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Nexpose™ configuration management system and associated documentation was performed. The evaluators found that the Nexpose™ configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well- developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Nexpose™ design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and

that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Nexpose™ during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Rapid7 LLC for Nexpose™. During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Nexpose™. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to Nexpose™ in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

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 TOE design was complete.

11.2 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.

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

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 is the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Creation of Sites: The objective of this test case is to confirm that the TOE provides the functionality to allow the global administrator to create additional sites[3] which can be assigned to specified users;

c. Creation of Asset Groups: The objective to this test case is to confirm that the TOE provides the functionality to allow the global administrator to create asset[4] groups which can be assigned to specified users;

d. Creation of Users: The objective of this test case is to confirm that the TOE provides the functionality to allow the global administrator to create additional users, and assign these users the roles of Security Manager, Site Owner, Asset Owner, and User;

e. Verify Administrative Privileges: The objective of this test case is to confirm that the TOE restricts administrative privileges to particular roles;

f. Verify Initial Site and Asset Group Assignments: The objective of this test case is to confirm that the TOE restricts access to the particular sites and asset groups that were set by the Global Administrator;

g. Modify Site and Asset Group Assignments for Users: The objective of this test case is to confirm that the TOE provides the capability to allow the Global Administrator to delete a Site and an Asset Group; and

h. Deletion of a User Account: The objective of this test case is to confirm that the TOE provides the capability to allow the Global Administrator to delete a user account. In addition, this case will also confirm that the deleted account is not able to authenticate to the TOE after it has been deleted.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

[3] A site is a collection of assets that are targeted for a scan.

[4] An asset is a single device on a network that Nexpose™ discovers during a scan.

a. Port Scanning. The objective of this test is to determine if there are any opened ports that could be exploited;

b. Cross Site Scripting. The objective of this test is to determine if there are any obvious Cross-Site Scripting vulnerabilities;

c. Concurrent Global Administrator Sessions. The purpose of this test case is to verify that the TOE manages concurrent administrator sessions successfully; and

d. SQL Injection. The purpose of this test case is to verify that the TOE is resistant to standard SQL injection attacks against its logon functionality.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Nexpose™ was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. 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 a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Nexpose™ behaves as specified in its ST and functional specification and TOE design.

12 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.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list

Acronym/Abbreviation/ Initialization	Description
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IP	Internet Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NSC	Nexpose™ Security Console
NSE	Nexpose™ Scan Engine
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

14 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1 Security Target, 1.7, 11 May 2012.

e. Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1, Version 1.3, 14 May 2012.