Certification Report

Pivotal tc Server Standard Edition

v2.8.2 RELEASE

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-240-CR
Version: 1.0
Date: 17 July 2013
Pagination: i to iii, 1 to 8

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 CGI IT Security Evaluation & Test Facility.

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 17 July 2013, 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 or registered trademarks:

- VMware is a registered trademark of VMware, Inc.

TABLE OF CONTENTS

Executive Summary

Pivotal tc Server Standard Edition v2.8.2 RELEASE (hereafter referred to as Pivotal tc Server), from Pivotal, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Pivotal tc Server is a web application based on open-source Apache Tomcat. The TOE provides Hypertext Transfer Protocol (HTTP), Apache JServ Protocol (AJP), and Java Management Extensions (JMX) interfaces through which users may connect. Authentication to the HTTP and AJP interfaces require a username and password combination that may be entered in either a form or a browser-based method. Access to JMX interface is restricted to those users on the same local area network as the TOE itself.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 14 June 2013 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 Pivotal tc Server, 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 2 *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: e.g. ALC_FLR.3 – Systematic Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Pivotal tc Server 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) 2 augmented evaluation is Pivotal tc Server Standard Edition v2.8.2 RELEASE (hereafter referred to as Pivotal tc Server), from Pivotal, Inc..

2 TOE Description

Pivotal tc Server is a web application based on open-source Apache Tomcat. The TOE provides Hypertext Transfer Protocol (HTTP), Apache JServ Protocol (AJP), and Java Management Extensions (JMX) interfaces through which users may connect. Authentication to the HTTP and AJP interfaces require a username and password combination that may be entered in either a form or a browser-based method. Access to JMX interface is restricted to those users on the same local area network as the TOE itself.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Pivotal tc Server is identified in Section 6 of the ST.

4 Security Target

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

Title: Pivotal, Inc. tc Server Standard Edition v2.8.2 Security Target
Version: 1.2
Date: 23 May 2013

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.*

Pivotal tc Server 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 in the EAL 2 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.

6 Security Policy

Pivotal tc Server implements an access control policy to control user access to the system; details of this security policy can be found in Section 6 of the ST.

In addition, Pivotal tc Server implements other policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TSF, resource utilization and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Pivotal tc Server 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 Assumption is listed in the ST:

- Administrators are non-hostile, appropriately trained, and follow all administrator guidance; and

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The connection between the two clustered instances of the TOE and any TOE environmental components (the Apache Web Server, Remote Administrator workstation) are all located within a controlled access facility on a secured network;
- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the Linux OS in the TOE environment (where the TOE is installed), other than those services necessary for the operation, administration, and support of the TOE;
- The TOE environment will provide physical security commensurate with the value of the TOE and the data it contains;
- The TOE software will be protected from unauthorized modification; and
- The TOE environment provides protection for the administration of TOE's Extensible Markup Language (XML) configuration files from unauthorized users.
- The TOE environment will be able to authenticate users with X.509 certificates as an authentication credential.

8 Evaluated Configuration

The evaluated configuration for Pivotal tc Server comprises:

The software Pivotal tc Server Standard Edition v2.8.2 RELEASE running on Java 1.7 on one of the following Operating Systems:

- Red Hat Enterprise Linux (RHEL) v5 or V6;
- Ubuntu 10.04 LTS;
- Windows Server 2008 SP2; and
- Windows Server 2003 SP2 and newer.

The publication entitled Pivotal Inc. tc Server Standard Edition v2.8.2 Guidance Supplement v0.4 describes the procedures necessary to install and operate Pivotal tc Server in its evaluated configuration.

9 Documentation

The Pivotal, Inc. documents provided to the consumer are as follows:

a. Getting Started with vFabric tc Server, VMware vFabric Cloud Application Platform 5.0, VMware vFabric tc Server 2.8,November 2012;
b. vFabric tc Server Administration, VMware vFabric Cloud Application Platform 5.0, VMware vFabric tc Server 2.8, October 2012;
c. tc Server 2.8 Release notes, March, 2013;
d. Apache Tomcat 7 Documentation (online); and
e. Pivotal Inc. tc Server Standard Edition v2.8.2 Guidance Supplement v0.4, May 23, 2013.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Pivotal tc Server, including the following areas:

Development: The evaluators analyzed the Pivotal tc Server 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 Pivotal tc Server security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Pivotal tc Server 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 Pivotal tc Server configuration management system and associated documentation was performed. The evaluators found that the Pivotal tc Server configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

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

The evaluators reviewed the flaw remediation procedures used by Pivotal, Inc. for the Pivotal tc Server. During a site visit, the evaluators also 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 Pivotal tc Server. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Pivotal tc Server potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Pivotal tc Server in its operational environment.

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

11 ITS Product Testing

Testing 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 analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

[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.

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.

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 CGI IT Security Evaluation & Test Facility 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. Identification, Authentication and Access Control: The objective of this test goal is to confirm the TOE's Identification, Authentication and Access Control meets the requirements of the ST;

c. User Lookout: The objective of this test goal is to confirm that the TOE will correctly enforce the session disconnect; and

d. Thread Quotas: The objective of this test goal is to confirm that the TOE properly enforces the maximum number of connections as claimed by the ST.

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:

a. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to reveal any potential avenues of attack;

b. HTTP Interface: The objective of this test goal is to verify exploits against HTTP interfaces;

c. Tomcat transfer: The objective of this test goal is to verify exploits against the Tomcat Transfer Encoding Module; and

d. Weak Passwords: The objective of this test goal is to confirm the TOE will not allow the usage of weak passwords.

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

11.4 Conduct of Testing

Pivotal tc Server 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 CGI IT Security Evaluation & Test Facility. 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 Pivotal tc Server behaves as specified in its ST and functional specification.

12 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.

13 Evaluator Comments, Observations and Recommendations

The evaluator notes that the usage of this product does not mitigate against a number of threats that would be encountered on an untrusted network. Potential consumers of this certification are encouraged to review the scope of the evaluation and the security claims that are made within the security target.

The evaluator also encourages potential customers to subscribe to product updates from the vendor. While the process of providing updates is possible to change in the future, the evaluator noted a robust infrastructure from a mature vendor for the mitigation of bugs and security flaws.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AJP	Apache JServ Protocol
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report

Acronym/Abbreviation/ Initialization	Description
HTTP	Hypertext Transfer Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JMX	Java Management Extensions
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
RHEL	Red Hat Enterprise Linux
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	Toe Security Functionality
XML	Extensible Markup Language

15 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. Pivotal, Inc. tc Server Standard Edition v2.8.2 Security Target, Security Target, version 1.2, 23 May 2013.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Pivotal, Inc. tc Server Standard Edition v2.8.2, version 0.6, 14 June 2013.