National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436)

Report Number: CCEVS-VR-VID10205-2009
Dated: 25 September 2009
Version: 3.5

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Sarah M Weinberg, Lead Validator

Mitre

Jandria Alexander, Senior Validator

The Aerospace Corporation

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary 4
2 Identification 5
3 Organizational Security Policy 6
3.1 User Data Protection 7
3.2 Security management 7
3.3 Protection of the TSF 7
4 Assumptions and Clarification of Scope 7
5 Architectural Information 8
6 Documentation 10
6.1 Design documentation 10
6.2 Guidance documentation 10
6.3 Configuration Management documentation 11
6.4 Delivery and Operation documentation 11
6.5 Life Cycle Support documentation 11
6.6 Test documentation 11
6.7 Vulnerability Assessment documentation 12
6.8 Security Target 12
7 IT Product Testing 12
7.1 Developer Testing 12
7.2 Evaluation Team Independent Testing 12
7.3 Penetration Testing 13
8 Evaluated Configuration 13
9 Results of the Evaluation 13
9.1 Evaluation of the Security Target (ASE) 14
9.2 Evaluation of the CM capabilities (ACM) 14
9.3 Evaluation of the Delivery and Operation documents (ADO) 14
9.4 Evaluation of the Development (ADV) 14
9.5 Evaluation of the guidance documents (AGD) 15
9.6 Evaluation of the Life Cycle Support Activities (ALC) 15
9.7 Evaluation of the Test Documentation and the Test Activity (ATE) 15
9.8 Vulnerability Assessment Activity (AVA) 15
9.9 Summary of Evaluation Results 16
10 Validator Comments/Recommendations 16
11 Security Target 16
12 List of Acronyms 16
13 Glossary of Terms 17
14 Bibliography 17

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436).

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 28 August 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL4 augmented with ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436). The TOE is designed to operate in the context IBM WebSphere Application Server and provide a platform supporting and controlling access to web-related objects.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436)
Protection Profile	Not applicable
ST	IBM WebSphere Portal 6.0 Security Target, Version 1.0, 23 September 2009
Evaluation Technical Report	Evaluation Technical Report For IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) Part 1 (Non-Proprietary), Version 3.0, 23 September 2009; Part 2 (Proprietary), Version 2.0, 28 July 2009
CC Version	Common Criteria for Information Technology Security Evaluation,

Item	Identifier
	Version 2.3, August 2005
Conformance Result	CC Part 2 extended and Part 3 conformant, EAL4 augmented with ALC_FLR.2
Sponsor	IBM Corporation
Developer	IBM Corporation
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Terrie Diaz, Eve Pierre
Validation Body	NIAP CCEVS: Sarah M Weinberg, Lead Validator Jandria Alexander, Senior Validator

3 Organizational Security Policy

This section summarizes the security functions provided by IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) that is evident at the various identified interfaces. It is based on information provided in the Security Target.

IBM WebSphere Portal (WP) is a Java 2 Enterprise Edition (J2EE) application executed in the run-time environment provided by WebSphere Application Server (WAS) version 6.0.2.29 that provides users a consistent view of portal applications and allows users to define specific sets of applications which are presented in a single context.

WP relies on TOE environment, the WAS, for the identification and authentication of authorized users. WP also relies on WebSphere Member Manager (WMM) to provide user profile information and group membership information to the TOE. The TOE environment establishes user sessions and maintains those sessions to keep user sessions separate from each other as well as to support the protection of the TOE..

WP allows authorized users to establish protected portal resources like pages and portlets. As an example, authorized users (a team) can develop, share, and store information for projects. This allows for fast access to and transfer of information between members of the team working on the same project.

The Access Control administration can be performed using corresponding portlets within the running portal, the XmlAccess interface, or via portal scripting.

3.1 User Data Protection

The TOE includes a Portal Access Control (PAC) mechanism that is invoked by the other TOE components to make access decisions for the following resources offered by WP: Web Modules, Portlets (Portlet Definitions), Portlet Application Definitions. Content Nodes (Pages), Application Templates, Template Categories, User Groups, URL Mapping contexts, Policies, and WSRP Producers. Access is controlled based on permissions contained in roles assigned to individual users or user groups. The other TOE components are responsible for enforcing the access decision made by the PAC mechanism.

3.2 Security management

The TOE supports roles defined as sets of resource specific permissions. Roles can be assigned to users, groups, and can also be aggregated into other (application) roles. Roles can be used to enable security management functions, such as managing roles and assigning those roles to users and user groups. In general, access to resources is restrictive insofar as a given user must have permission before they can access a resource. While it is possible to authorize anonymous access to a resource, such permission must be explicitly established prior to so doing.

The TOE also provides the ability to log the use of the security management functions. While generated by the TOE, the log is stored in ASCII format in a file in the IT environment.

3.3 Protection of the TSF

The TOE ensures that its own security policies cannot be bypassed by ensuring that appropriate access checks are made and enforced at all interfaces made available by the TOE.

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed that there are one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile.
- It is assumed that the applications that the TOE relies upon, have been configured in accordance with the manufacturer's installation guides and where applicable, in its evaluated configuration. It is securely configured such that the applications protect the TOE from any unauthorized users or processes.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- The right to access a resource is determined on the basis of: the user groups the user is a member of; the role instances assigned to those user groups or to the user; the role instances contained in application roles assigned to those user groups or to the user; the permissions contained in the individual assigned role instances which are determined on the basis of the actions contained in the corresponding role type and the set of descendant resources in the role domain which is determined in the basis of the topology defining the parent child relation ship among the resources and the role blocks that exist on those resources; and, the set of resources owned by the user or the user groups the user is a member of.

PAC is the single access control decision point within the TOE. It controls access to all sensitive portal resources. Protected resources are resources that can be accessed by a restricted set of users only. In order to be granted access to a protected resource in a specific way, the user needs a corresponding permission on this resource, e.g. a specific portal page can only be viewed by a specific user, if the user has the permission to perform the action 'View' on that page. Note that this discussion focuses on the PAC only because it is the central access control decision maker utilized by all other components of the TOE.

5 Architectural Information[1]

The TOE is the IBM WebSphere Portal (WP) product. Its boundaries are primarily defined by the interfaces offered to the resources to which it controls access and the other components upon which it relies for supporting services.

The WP allows authorized users to establish protected portal resources. As an example, authorized users (a team) can develop, store, and share information for projects. This then allows for fast access to and transfer of information between members of the team working on the same project.

The WP provides the access control to protected resources. Access control checks are implemented specifically by the Portal Access Control (PAC) component within WP. This is shown within the figure below, which illustrates that PAC is the common point of access control. While the PAC makes all the access decisions, the other WP components, as identified in the figure below, are responsible to enforce the decisions of the PAC so that the access control is effective (i.e., not bypassable). As such, all the components of WP cooperate to instantiate the TSF.

When a user requests access to a resource from the web browser, the WP relies upon IT Environment, specifically the WebSphere Application Server (WAS), to perform identification and management of users, WebSphere Member Manager (WMM) to provide the group membership and a database for the mapping of users to roles and the actions to resources. The request is passed to the TOE via the PAC to make an access decision to be enforced by the other applicable (depending on the specific service being invoked) WP components. Neither WAS or WMM are within the scope of evaluation and are therefore

[1] Extracted from SAIC Final ETR Part 1 Version 3.0, 23 September 2009

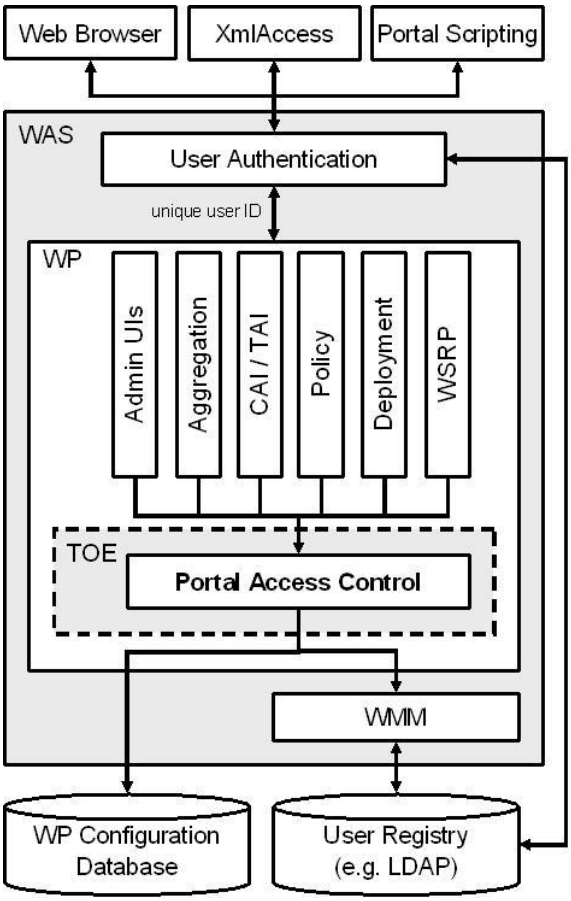
part of the TOE environment. WP also relies upon WAS and a database for its own proper and secure operation. More specifically, it is expected that the operating environment provided by the underlying WAS will serve to protect the execution environment of WP and the database will serve to protect the WP data so that it is accessible only by WP. In general, WP expects WAS and WMM to protect against attempts, outside the control of the TOE, at tampering with or bypass of the TOE security functions.

The figure below shows the PAC component as the central point of access control. The main interfaces to TOE, which are exposed through the various WP components, are:

- The Administration (Admin) Portlets[2] ;
- XmlAccess
- Portal Scripting

Admin portlets are the GUI Administration interface operated through a Web Browser. XmlAccess is a command line tool that allows importing and exporting portal configuration data from and to XML documents. Portal Scripting is an interactive command line tool for WP administration similar to an operating system command line shell.

[2] Portlets are the heart of a portal. A portlet is a small application window, usually depicted as a small box in a web page. Portlets are re-usable UI components that provide access to backend business logic, web-based content and other resources or services. Portlets can be grouped together in a portlet application. Portlets run inside the portlet container of WP, similar to a servlet running on an application server.



6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

6.1 Design documentation

Document	Version	Date
WP 6.0 Portal Access Control System Design and Architecture Document		4/07/2009
Representation Correspondence Documentation IBM WebSphere Portal 6.0		2/19/2009
WebSphere Portal 6.0 Security Policy Model	Revision 0.1	December 06, 2007

6.2 Guidance documentation

Document	Version	Date
IBM WebSphere Portal 6.0 Administration	Version 6.0	

Document	Version	Date
online at IBM http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp		
IBM WebSphere Portal 6.0 Installation and Configuration	Version 6.0	
Addendum for Portal 6.0.0.0 Common Criteria	Version 1.0	July 15, 2009

6.3 Configuration Management documentation

Document	Version	Date
IBM WebSphere Portal 6.0, Configuration Management Plan	Version 0.5	February 27, 2009

6.4 Delivery and Operation documentation

Document	Version	Date
IBM WebSphere Portal 6.0 Delivery and Operation	Version 0.2	March 31, 2008
IBM WebSphere Portal 6.0 Installation and Configuration	Version 6.0	
Addendum for Portal 6.0.0.0 Common Criteria	Version 1.0	July 15, 2009
DSW Secure Media Delivery (SMD)	v1.0	
Download Director Applet Functional Specification	Version 6.00	February 5, 2004
Tequila Functional Specification	Version 3.01	December 16, 2003

6.5 Life Cycle Support documentation

Document	Version	Date
IBM WebSphere Portal 6.0 Life Cycle Support	Version 0.5	February 27, 2009
Security Standards for Essential Network and Computing Services ITCS204	Version 4.3	March 31, 2003
AS Security Admin ITCS314	Version 1.0	December 31, 2002

6.6 Test documentation

Document	Version	Date
IBM WebSphere Portal EAL4 Developer Testing	Version 1.15	7/13/09

The actual test results have been submitted to the evaluation team in various log files.

6.7 Vulnerability Assessment documentation

Document	Version	Date
IBM WebSphere Portal 6.0.0.0 with APARs[1] PK67104 and PK79436 Vulnerability Assessment	Version 0.85	July 18, 2009

6.8 Security Target

Document	Version	Date
IBM WebSphere Portal 6.0 Security Target	Version 1.0	9/23/09

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security User Data Protection, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire developer's automated test suite on AIX, Linux RedHat, and Windows Server 2003. In addition to re-running the developer's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the developer's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the TOE software for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
  - Any hardware that supports the TOE components is acceptable.
- IT Environment Hardware
  - Any hardware that supports the non-TOE IT components is acceptable.
- Test Hardware
  - Squash Server
  - Squash Clients
  - Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment.

The following software is required to be installed on the machines used for the test:

- TOE Software

    - IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436)
- IT Environment Software
    - Windows 2003 Standard Edition with Service Pack 1
    - Red Hat Enterprise Linux (RHEL) Advanced Server (AS) V4.0
    - AIX V5.3 ML02
    - WebSphere Application Server (WAS) version 6.0.2.29
    - WebSphere Member Manager (WMM)
    - Microsoft Internet Explorer 7.0
- In addition, the following software is required in support of the test cases:
    - J2EE Squash application
    - Borland SilkTest
    - SquashAgent
    - Automated Test Harness

7.3 Penetration Testing

The evaluators developed penetration tests to address Web Application Vulnerabilities, such as information leakage and improper error handling, injection flaws, and Cross Site Scripting (XSS), Broken Authentication and Session Management, Failure to Restrict URL Access, C.4.4 Access problems with BasicAuthTAI, and C.4.5 Environment Vulnerabilities. The evaluator also expanded upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The TOE is WebSphere Portal 6.0 provided by IBM, which is designed to operate in the context IBM WebSphere Application Server and provide a platform supporting and controlling access to web-related objects.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on February 2007. The evaluation confirmed that the IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL4 Augmented with ALC_FLR.2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436), Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the IBM WebSphere Portal 6.0 Security Target, Version 1.0, dated 23 September, 2009.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 4 augmented with ALC_FLR.2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control, and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from IBM.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 4 augmented with ALC_FLR.2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

The evaluation team followed the WebSphere® Portal Installation and Configuration Version 6.0 and IBM WebSphere Portal 6.0 Administration to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 augmented with ALC_FLR.2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the

correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 4 augmented with ALC_FLR.2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The WebSphere® Portal Installation and Configuration Version 6.0, IBM WebSphere Portal 6.0 Administration, and Admin Supplement were assessed during the design and testing phases of the evaluation to ensure it was complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL4 augmented with ALC_FLR.2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE. To support the ALC evaluation, the evaluation team performed a Life Cycle audit at the IBM facility in Research Triangle Park (RTP), NC. During the audit, the evaluation team witnessed the use of the security measures as described in the Life Cycle documentation and sampled records created by using the security procedures.

In addition to the EAL4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 4 augmented with ALC_FLR.2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 4 augmented with ALC_FLR.2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, the evaluation team's misuse analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR. The validation team therefore recommends that the evaluation results be accepted. The components in the IT environment, including the WAS and the WMM, are not included in this evaluation. As such, their security functionality and assurance must be assessed separately.

The TOE does not meet the CC defined FAU_GEN SFR. However, the TOE does meet explicitly stated requirement, "Logging of security management functions" (FMT_LOG_EX.1), which supports the auditing of security management functions.

11 Security Target

The Security Target is identified as IBM WebSphere Portal 6.0 Security Target, Version 1.0, 23 September, 2009. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL4 augmented with ALC_FLR.2.

12 List of Acronyms

ACL Access Control List

API Application Programming Interface

CC Common Criteria

CM Configuration Management

EAL Evaluation Assurance Level

FIPS Federal Information Processing Standard

IBM International Business Machines

ID Identification

IT Information Technology

NIST National Institute of Standards and Technology

PC Personal Computer

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

XML Extensible Markup Language

13 Glossary of Terms

See the Glossary of definitions already defined by the ST, CC, or CEM

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) Final Proprietary ETR – Part 2, Version 2.0 dated 28 July 2009 and Supplemental Team Test Report, Version 2.0, 28 August 2009.

[6] IBM WebSphere Portal 6.0.0.0 (with APAR PK67104 and APAR PK79436) Non-Proprietary ETR – Part 1, Version 3.0, 23 September 2009.

[7] IBM WebSphere Portal 6.0 Security Target, Version 1.0, 9/23/09.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.