National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

AquaLogic® Interaction Publisher 6.4 MP1 Patch 1

Report Number: CCEVS-VR-10107-2009
Dated: 20 February 2009
Version: 1.2

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

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the AquaLogic® Interaction Publisher 6.4 MP1 Patch 1 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in January 2009. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 2.3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

Publisher is a web-based software application that functions as a remote server of AquaLogic Interaction (ALI) to provide the services required to deploy content-driven applications, such as a customer support knowledge base or sales support center, where users can create and manage Web content without HTML skills. Publisher is not a stand-alone product; rather it integrates directly with ALI and depends on ALI portal pages and security functions. ALI, in turn, is the base portal application and framework for the AquaLogic User Interaction (ALUI) product family. ALI integrates custom-developed applications and ALUI components into a cohesive web-based work environment that is viewed from a user's web browser.

Publisher is supported in the following environments:

- Operating systems (OS)—Microsoft Windows Server 2003 SP1; Solaris 10 (on SPARC); and Red Hat Enterprise Linux 4 Update 3 (x86)
- Application servers— JBoss Application Server, version 3.2.7 (bundled and installed with Publisher)
- Database servers—Microsoft SQL Server 2005 (with SQL Server 2000 compatibility level); and Oracle 10g R2 (10.20.1 and above) in default or Oracle RAC configuration
- Web browsers—Internet Explorer 6.0 SP2 and 7; Firefox 1.5.

The TOE is dependent on the correct operation of the environment and on its underlying OS, neither of which are included within the scope of the evaluation. It should also be noted that the access control policy implemented by the TOE is enforced only on access attempts made through the TOE's interfaces. The TOE does not and cannot control attempts to access data directly (e.g., via the underlying OS).

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the BEA AquaLogic Interaction Publisher 6.4 MP1 Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	AquaLogic® Interaction Publisher 6.4 MP1 Patch 1
Sponsor:	BEA Systems, Inc 475 Sansome Street San Francisco, CA 94111
Developer:	BEA Systems, Inc 475 Sansome Street San Francisco, CA 94111
CCTL:	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Kickoff Date:	June 27, 2005
Completion Date:	13 January 2009
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.3, August 2005.
Evaluation Class:	EAL 2 augmented with ALC_FLR.2
Description:	AquaLogic® Interaction Publisher 6.4 MP1 Patch 1 is a web-based software application that functions as a remote server of AquaLogic® Interaction (ALI) to provide the services required to deploy content-driven applications. The TOE consists of the following components: Content Web Application; Workflow Web Application; and Image Service Files.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the AquaLogic® Interaction Publisher 6.4 MP1 Patch 1 product by any agency of the U.S. Government and no warranty of the Publisher product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Lisa Vincent

Validation Body: National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE is intended to counter.

T.ACCESS	A user may gain unauthorized access to the TOE and the TOE's protected objects.
T.MANAGE	A user may gain unauthorized access to the utilities available to manage the security-related functions of the TOE.

2 Identification

The evaluated product is **AquaLogic® Interaction Publisher 6.4 MP1 Patch 1.**

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the Publisher security policy has been extracted and reworked from the AquaLogic Interaction Publisher 6.4 MP1 ST and Final ETR.*

3.1 User Data Protection

Publisher defines a role-based access control policy to control the users that can access and act upon the TOE defined objects. This access control policy works in conjunction with the access control policy defined in ALI. The users of the TOE are defined, managed and maintained by ALI.

3.2 Security Management

Publisher provides the authorized administrator an interface to manage access control attributes, assignment of roles, and security-related functions as 'folder-level' security that supplements the security provided by ALI. The TOE depends upon ALI to define the administrators of the TOE.

3.3 Protection of the TSF

Publisher enforces the access control policy to ensure that the security functions cannot be bypassed. Publisher depends on its operating environment to store and protect its data and ensure that its security functions are not tampered with or bypassed. Publisher leverages the security functions offered by ALI to ensure that users are identified and authenticated before access to Publisher is granted. Publisher depends upon ALI to define, maintain, and manage its administrator groups, and the users, user groups, and community members that can be assigned to Publisher roles.

4 Assumptions

The following assumptions are identified in the ST:

Table 2 – Assumptions

Assumption Identifier	Assumption Description
A.AUTH_USERS	Only the users authorized to access the information within the TOE may access the TOE.
A.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner to maintain to the IT security objectives.
A.NOEVIL	The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.
A.PHYSICAL	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.
A.OPE_ENV	The TOE operating environment shall provide the mechanism to isolate the TOE components and resources, ensure the TOE cannot be tampered with or bypassed and the TOE data is protected from unauthorized deletions.
A.TRANSMIT	The operating environment will protect the data transmitted to and from the TOE.
A.USER	The authorized users are not negligent or malicious and will follow the guidance provided.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is AquaLogic® Interaction Publisher 6.4 MP1 Patch 1, henceforth referred to as Publisher.

The TOE is dependent on the correct operation of the environment, including the AquaLogic Interaction (ALI) product and its underlying OS, neither of which are included within the scope of the evaluation (although it should be noted that BEA AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0 has been successfully evaluated at EAL2 augmented with ALC_FLR.2). It should also be noted that the access control policy implemented by the TOE is enforced only on access attempts made through the TOE's interfaces. The TOE does not and cannot control attempts to access data directly (e.g., via the underlying OS).

5 Architectural Information

The Target of Evaluation (TOE) is AquaLogic® Interaction Publisher 6.4 MP1 Patch 1, henceforth referred to as Publisher.

Publisher is a web application that functions as a remote portlet server for AquaLogic Interaction (ALI). Publisher enables content creation, content publishing, and workflow management. TOE operation requires AquaLogic Interaction.

Publishing makes content available to end users as web pages. Publisher enables users to:

- Publish content to published content portlets, to the ALI Knowledge Directory, or to an external web site
- Publish content immediately or schedule it to be published at a later date
- Preview content before publishing it to confirm layout and appearance according to pre-defined presentation templates
- Publish content to the ALI Knowledge Directory using a Publisher content crawler
- Remove published content from the web server by setting it to *expire*. This removes it from the web server but keeps it in the Publisher directory. Users can set a published content item to expire immediately or schedule a future expiration.

Publisher's web publishing functions enable users without HTML skills to create and manage web content. Publisher supports the definition of structured content types; web browser form-based data entry; and publishing of content by combining data values with a text presentation template and copying the result to a file system or FTP server.

Publisher integration with ALI uses several ALI functions including the following:

- User and group management
- Document storage and management
- Content search
- Object security
- User identification and authentication.

Within the TOE, data is organized in a directory structure using folders. Publisher interfaces are used to add, edit, organize, preview and publish content. The core building block of Publisher content is the content item. Publisher provides the following features:

- Data Entry Templates—content items can be created based on data entry templates. These templates define the properties available for creating a content item
- Presentation Templates—these templates enable the definition of standardized pages with consistent branding. The presentation template determines the appearance and format of a content item when it is published to the web server. Data entry templates are always associated with a presentation template
- Published Content Portlets—published content portlets present content through ALI and can enable users to submit and edit content
- Published content portlet templates—published content portlet templates enable a user without HTML skills, such as a community manager, to create published content portlets. Publisher provides sample portlet templates that can be used as-is or modified to meet an organization's needs. Users can also create their own portlet templates from scratch

- Content items—content items are the base objects that are managed using Publisher. A content item can be a set of values or an uploaded document or image file
- Publisher Explorer—this is the central interface for viewing and managing Publisher objects, including content items, data entry templates, and presentation templates. Publisher Explorer enables users with administrative roles to set up and manage a folder structure to organize content items and published content portlets, and to assign security roles to users and groups by folder
- Workflow—the workflow function enables an organization to manage the review, approval, and publishing of content using structured and repeatable processes. Authorized users define workflows, which consist of an ordered list of workflow activities, each of them assigned to a user or group of users. Publisher provides portlets that enable tracking of personal workflow assignments and content items in workflow by folder
- Scheduled publishing and expiration—enables users to schedule content publishing and automatically remove content from publishing targets and the ALI search index.

Publisher consists of the following core components:

- Publisher—a Java servlet-based web application providing the logic and the bulk of the user interface functionality for the creation and maintenance of content and for linear workflows that can be used to govern the approval and publishing of content. With one exception (a diagnostics page), all user interfaces are in the form of portlets that require ALI for display. Publisher includes administrative and content-related portlets and configuration wizards, including the Administer Publisher portlet. These portlets are added to and accessed from the ALI portal pages, but the functionality is provided and controlled by Publisher
- Image Service Files—these required files provide the necessary images, styles, user interface controls, Java applets, and online help for Publisher. These files are integrated with the ALI's Image Service.

The Publisher component in turn comprises the following subsystems:

- Content Web Application Subsystem—this is implemented as two layers: a user interface layer; and an API layer:
  - The user interface layer renders the GUI displayed to the user of Publisher via the portlets hosted in ALI. The user interface layer performs initial checks of the user's role and permissions in order to render the appropriate items and menus. However, all security checks for permitted operations eventually are performed in the API layer
  - The API layer performs the security checks for the logged in user and the requested operation.
- Workflow Web Application Subsystem—comprises the following main components:
  - Workflow engine—a J2EE process execution engine that keeps track of the state of all content items governed by workflows, and that responds to initiation/approval/rejection events by updating the state
  - Workflow pages—user interface pages for creating new workflows, viewing a user work list of activity assignments, and viewing content items governed by workflows.

The TOE depends on its operating environment to store and protect user and TSF data and ensure that the TOE functions are not tampered with or bypassed. The TOE leverages the security functions offered by ALI to ensure that users of the TOE are identified and authenticated before access to the TOE is granted. The TOE depends upon ALI to define, maintain, and manage the administrator groups of the TOE, and the users, user groups, and community members that can be assigned to the roles in the TOE.

The TOE implements user data protection by applying a role-based access control policy to folders in the folder hierarchy. All objects within a folder are subject to the access controls applied to the containing folder.

The TOE supports security management by defining security management roles and restricting security management activities to defined roles.

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

- BEA AquaLogic® Interaction Publisher Administrator Guide, Version 6.4, 20 Feb 2008
- BEA AquaLogic® Interaction Publisher Installation and Upgrade Guide, Version 6.4, 11 Apr 2007
- BEA AquaLogic® Interaction Publisher Online Help

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for AquaLogic® Interaction Publisher 6.4 MP1 Patch 1.

Evaluation team testing was conducted at the vendor's development site May 27 through May 30, 2008.

7.1 Developer Testing

BEA's approach to testing for Publisher is based on TOE Security Function (TSF) interface testing. BEA has developed a test suite comprising various manual tests to exercise the TSF at the user interfaces as described in the TOE Functional Specification. The vendor addressed test depth by analyzing the functionalities addressed in the high-level design and associating test cases that cover the addressed functionalities. The high-level design addressed the general functions of the TOE subsystems, identifying the security functionality of each subsystem, as appropriate. The testing documentation maps security functions to specific test suites and tests, while the development documentation maps security functions to subsystems. The combination of the two mappings shows how the tests map to the subsystems.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the operating systems supported and the application environment. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed the vendor test suite for Publisher per the evaluated configuration as described in the AquaLogic Interaction Publisher 6.4 Testing Documentation (ATE) document. Section 3 (Test Environment and Setup Procedures) of the Testing Documentation describes the testing environment for Publisher as the JBoss Application Server version 3.2.7 running on one of: Microsoft Windows Server 2003 SP1; Solaris 10 (SPARC); or Red Hat Enterprise Linux 4.0 update 3; with AquaLogic Interaction 6.1 MP1 in one of the following three testing configurations:

- Microsoft Windows Server 2003 SP1 using Microsoft Internet Information Service (IIS), Version 6.0 with .NET 1.1 SP1 [and co-existence with .NET 2.0] and Microsoft SQL Server 2005 (with SQL Server 2000 compatibility level)
- Solaris 10 (SPARC) with BEA WebLogic Server 9.2 with Sun Java 2 JDK 5.0 with the Java HotSpot™ Client and Server VMs (32-bit), version 1.5.0_06 and Oracle 10G R2 (10.2.0x).
- Red Hat Enterprise Linux 4.0 update 3, BEA WebLogic Server 9.2 with BEA JRockit 5.0 (R26.0.0) JDK (32-bit) and Oracle 10G R2

In addition, each testing configuration requires either of the following Web browsers: Internet Explorer 6.0 SP2 or Mozilla Firefox 1.5.

The evaluation team conducted testing of Publisher on the Red Hat Linux environment as described above. In parallel, the evaluation team conducted testing of AquaLogic Interaction Collaboration on a Windows Server 2003 SP1 environment (see CCEVS-VR-VID10104-2009 for information about this testing). Since Publisher's direct reliance is on the JBoss Application Server, regardless of underlying operating system, this was deemed sufficient coverage. Collaboration is similarly dependent on a single application server (in this case, Tomcat Server 5.0.28), so these two TOEs were tested with the supporting ALI TOE in different supported configurations. The evaluation team used Internet Explorer 6.0 SP2 as the browser in the test environment.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environment described above was used with team generated test procedures and team analysis to determine the expected results.

The evaluation team performed the following additional functional tests:

- **Confirmation of Role Permissions**—Table 6-1 of the ST identifies the permissions associated with each role defined in the access control policy (i.e., Administrator, Folder Administrator, Producer, Editor, Contributor, Submitter, and Reader). Several of the developer's tests include steps to confirm that a user in a specific role is restricted to the appropriate functions, consistent with the information in Table 6-1. However, there did not appear to be a single, comprehensive test that confirms that a user is appropriately restricted. The evaluation team confirmed that each role is restricted to the capabilities defined in Table 6-1 of the ST
- **Use of Settings by Publisher**—An outcome of the Final VOR for the ALI evaluation (VID10103) was for the evaluation team to examine the use of settings by the dependent TOEs (i.e., Publisher (VID10107) and Collaboration (VID10104). The evaluation team examined the configuration of Publisher portlets and web services and determined only one web service was configured to use Administrator settings. Further testing confirmed the ability to modify the Administrator settings is constrained to TSF interfaces that control access and restrict it to users with administrative rights

- **Self protection and non-bypassability**—the developer's test coverage analysis did not specifically trace any tests to the TSF Protection security function. However, a number of the developer's tests appeared to exercise this functionality. The developer's tests demonstrated that all requests to access a TOE object are mediated by the TOE before access is granted. The developer's tests also demonstrated that restrictions on security management capabilities are enforced. The evaluation teams' testing demonstrated that attempts to access TOE objects or security management utilities using previously saved URLs from an administrative user session are also subject to access and permission checks, which are applied to the correct user.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product that searched five (5) additional well known vulnerability web sites and extended the search parameters used by the developer. The evaluation team did not discover any new open source vulnerabilities/bugs that pertain to the TOE that have not been corrected. The evaluation team conducted the following additional penetration tests for the reasons specified:

- **Navigate to unauthorized functions**—the authorized administrators access the TOE via a web-based interface. The purpose of this test is to enter into the Address field of the user's browser addresses of interface screens that the user is otherwise unauthorized to access to determine that the TSF can appropriately restrict access to TOE security management functions. The test demonstrates that the TOE performs checks that access is being attempted via the remote gateway
- **Replay vulnerability**—During the validation of the AquaLogic Interaction TOE (VID10103), and as a result of an investigation performed by the evaluation team in response to validator questions, the evaluation team identified that remote servers that were integrated with AquaLogic Interaction via a portlet were potentially susceptible to replay attacks. This vulnerability was not applicable directly to the evaluated version of AquaLogic Interaction, as it does include remote servers. However, Publisher 6.4 is deployed as a remote server of AquaLogic Interaction, and so was potentially vulnerable. The test demonstrated that a user able to access a browser session previously used by an Administrator, within a reasonable period of time, could reuse URLs to exploit the replay vulnerability and essentially perform some action as if they were the Administrator.

7.4 Post-Testing Activities

As a result of evaluation team testing, and the identification that the TOE was susceptible to a replay attack, the developer modified the TOE to implement more robust session termination. The developer provided the evaluation team with updated test evidence demonstrating the fix addressed the vulnerability identified by the evaluation team.

8 Evaluated Configuration

The evaluated version of the TOE is AquaLogic® Interaction Publisher 6.4 MP1 Patch 1.

Publisher is a web-based software application that functions as a remote server of AquaLogic Interaction (ALI) to provide the services required to deploy content-driven applications, such as a customer support knowledge base or sales support center, where users can create and manage

Web content without HTML skills. Publisher is not a stand-alone product; rather it integrates directly with ALI and depends on ALI portal pages and security functions. Publisher executes on JBoss Application Server version 3.2.7, which is bundled with Publisher as a convenience to the customer, but is not included within the scope of the evaluation. ALI is the base portal application and framework for the BEA AquaLogic User Interaction (ALUI) product family. ALI integrates custom-developed applications and ALUI components into a cohesive web-based work environment that is viewed from a user's web browser. Table 2-1 in the ST lists the IT environment components for Publisher.

9 Results of the Evaluation

The evaluation was conducted based upon version 2.3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.2" certificate rating be issued for AquaLogic® Interaction Publisher 6.4 MP1 Patch 1.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_FLR.2	Flaw Reporting Process
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis

AVA_VLA.1	Vulnerability analysis

10 Validator Comments/Recommendations

Note that there are no security functional requirements for collection of audit data. The start of this evaluation predates the CCEVS policy to require audit, if the evaluation began today this would not be permitted.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **AquaLogic Interaction Publisher 6.4 MP1 Patch 1 Security Target,** Version 1.0, dated 27 June 2008.

13 Glossary

The following acronyms beyond those in the CC or CEM are supplied; however, no additional definitions are supplied:

- **ALI –** AquaLogic Interaction
- **ALUI –** AquaLogic User Interaction
- **IDK –** Interaction Development Kit
- **J2EE –** Java2 Platform, Enterprise Edition
- **JDK –** Java Development Kit
- **LDAP –** Lightweight Directory Access Protocol
- **SOA –** Service Oriented Architecture
- **SOAP –** Simple Object Access Protocol
- **UI –** User Interface

14 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- BEA Systems, Inc. (http://www.bea.com)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005
- *Common Evaluation Methodology for Information Technology Security*, version 2.3, August 2005.

Other Documents:

- *AquaLogic Interaction Publisher 6.4 MP1 Patch 1 Security Target*, Version 1.0, 27 June 2008.