National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

BEA AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0

Report Number: CCEVS-VR-VID10103-2008
Dated: 23 May 2008
Version: 1.0

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 BEA AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic Interaction® Development Kit 6.0 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed on 14 March 2008. 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.

ALI with IDK is a sensitive data protection Web-portal server platform that provides users a single point of access to applications and information in a single unified interface. ALI includes a portal infrastructure, a user interface (UI), a document content management system and a search function that integrates applications and AquaLogic User Interaction (ALUI) components into a cohesive Web-based environment that can be customized and personalized to meet the internal and customer-oriented portal needs of large enterprise companies. IDK offers Java platform and .NET client-side libraries that provide connectivity to Web services-based application programming interfaces (APIs) for ALI.

ALI and IDK[1] are 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—Microsoft deployment with Microsoft IIS 6.0 with .NET Framework 1.1 SP1; Solaris deployment 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 for the Linux deployment with BEA WebLogic Server 9.2 with BEA JRockit 5.0 (R26.0.0) JDK (32-bit)
- 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
    - Administrative Users—Internet Explorer 6.0, Firefox 2.0
    - Browsing Users—Internet Explorer 6.0; Firefox 1.5, 2.0
- External authentication sources—LDAP; or Active Directory.

[1] IDK requires the same OS, application server and web browsers as the ALI but is set up on a separate platform used for customizing applications to import to the ALI component of the TOE.

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 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0 Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	BEA AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0
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:	March 14, 2008
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:	BEA AquaLogic Interaction 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0 is a Web-portal server platform that provides users a single point of access to applications and information in a single unified interface. The TOE consists of the following components: Portal server; Administrative Portal; Services (Automation, Content Upload, Document Repository, API, Search); ALI Logger; and the Image Service support component.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the BEA AquaLogic Interaction 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0 product by any agency of the U.S. Government and no warranty of the ALI Platform 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 Organizational Security Policies

The ST identifies the following organizational security policies with which the TOE is intended to comply.

P.ACCESS	The TOE must restrict the access to the TOE protected objects.
P.ACCOUNTABILITY	Users shall be held accountable for specific security relevant actions within the TOE.
P.AUTH_USERS	Only those users who have been authorized to access the information within the TOE may access the TOE.
P.MANAGE	The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the TOE.

2 Identification

The evaluated product is **BEA AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0.**

3 Security Policy

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

> ***Note:*** *Much of the description of the ALI with IDK security policy has been extracted and reworked from the BEA AquaLogic Interaction 6.1 MP1 with AquaLogic Interaction Development Kit 6. ST and Final ETR.*

3.1 Security Audit

ALI provides the capability to generate audit records, determine which user actions will be audited, and display the audit records. ALI is dependent upon the IT environment to store and protect the audit records from unauthorized modifications and deletions.

3.2 User Data Protection

The primary security functionality of the TOE is to provide access control to ALI resources. ALI enforces an access control policy based on access control lists (ACLs) to control users' access to ALI objects and administrative interfaces.

3.3 Identification and Authentication

ALI includes the capability to use third-party authentication sources such as Microsoft Active Directory and various LDAP 2.2 products to get user information and to perform identification and authentication. ALI enforces the identification and authentication decision received from the third-party source. ALI also includes an internal identification and authentication mechanism which is used to log in administrative users and users that are defined within ALI. ALI includes the capability to monitor the login process and lockout user accounts that exceed the configured unsuccessful login limit.

3.4 Security Management

ALI includes the Administrative Portal that is used by authorized administrators to manage the security functions of the TOE, including: management of the access control function and ACLs; management of the audit function; management of user accounts, groups and roles; and management of user authentication and authentication failure handling.

3.5 Protection of the TSF

ALI ensures all requests made through its interfaces to access its objects are mediated by the access control security function before any access is granted.

4 Assumptions

The following assumptions are identified in the ST:

Table 2 – Assumptions

Assumption Identifier	Assumption Description
A.INSTALL	Those responsible for the TOE must ensure the TOE is delivered, installed, managed, and operated in a manner that maintains 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 in the administrative guidance.
A.PHYSICAL	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.
A.OPE_ENV	The operating environment must protect the TOE and its resources from unauthorized deletions and tampering and provide a reliable timestamp for the TOE's use.
A.TRANSMIT	The operating environment will protect the data transmitted from the TOE to other IT products.
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 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0, henceforth referred to as ALI and IDK respectively.

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).

5 Architectural Information

The Target of Evaluation (TOE) is AquaLogic Interaction 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0, henceforth referred to as ALI and IDK respectively.

ALI is the portal platform for the BEA AquaLogic User Interaction (ALUI) suite of products. A portal is a Web site that gives users a single point of access to applications and information in a single unified interface. ALI includes a portal infrastructure, a user interface (UI), a document content management system, and a search function. ALI integrates applications and ALUI components into a cohesive Web-based environment that can be customized and personalized to meet the internal and customer-oriented portal needs of large enterprise companies.

The IDK offers Java platform and .NET client-side libraries that provide connectivity to Web services-based application programming interfaces (APIs) for ALI.

ALI's portal framework integrates applications by using portlets and also supports virtual community workspaces. Portlets are one of the mechanisms that end users use for accessing data

and applications from portals. Portlets enable the integration of functionality from external systems in the portal page, thus providing a single entry point (or window) for a wide range of content and services. Portlets can be used for everything from displaying useful information to building integrated applications that combine functionality from multiple systems. The ALI portlet architecture conforms to Service-Oriented Architecture (SOA) and leverages the key SOA interfaces and protocols: HTTP and SOAP. SOA is an IT strategy that organizes the discrete functions contained in enterprise applications into interoperable, standards-based services that can be combined and reused quickly to meet business needs.

Most of the ALI portal's end-user and administrative functionality and tools are packaged and implemented as portlets. ALI organizes this functionality into categories and implements each category in a set of portlets. The categories include the following:

- User Interface
- Web Services
- User Management
- Content management
- Security
- Search
- Scheduled Operations.

Separating the portlet UI from its application logic through a web service interface enables portability and supports ALI's capability to deploy on both J2EE and .NET web environments. Thus, ALI portlet architecture is characterized by the following:

- A front end that implements the portlet's UI
- A back-end that implements the portlet's functionality
- An interface between the front-end and the back-end (often a web service) that generates standard HTML or text output, including but not limited to complete web pages, XML data, or snippets of HTML.

The back end for a portlet can be any web application that returns HTML or XML over HTTP. Portlets can be coded in any language that communicates over HTTP. The code returned by a portlet is parsed by the portal and inserted into the appropriate cell in the HTML table that makes up every portal page. Most portlets are hosted remotely. Each portlet is self-contained and executes its particular functionality in its own process.

The IDK APIs (included with both the Java and .NET versions of the IDK) provide support for portlet development, including manipulating settings, accessing user information, and managing communication with the portal. Security is enforced by the portal in exactly the same way as when the functionality is executed from within the portal. In the ALUI web services architecture, most portlets are hosted remotely and connect to a back-end application for data or functionality. The remote portlets can access an API provided by the IDK called the Programmable Remote Client (PRC). The PRC API provides interfaces to perform object-oriented access into the portal's SOAP API, which expose elements of the portal API.

The IDK also enables developers to create remote authentication services. The IDK Authentication API provides an abstraction from the necessary SOAP calls and enables developers to simply implement an object interface for the external authentication service.

ALI consists of the following core components:

- Portal server and Administrative Portal – The following components run on an application server:
  - Portal server – Hosts the dynamically-generated Web pages that users view in the portal. This is the core component of ALI.
  - Administrative Portal – This component provides a centralized management user interface for setup, configuration, security, and other administrative activities.
- Services – The following support components run as Microsoft Windows services or Unix daemon processes depending on the deployment platform:
  - Automation Service – Manages job scheduling for portal administration and maintenance activities. These jobs can include custom jobs created by portal administrators and developers that access remote content services and identity services that store and retrieve information in the portal database.
  - Content Upload Service – The Content Upload Service enables the manual upload (or automatic crawling) of document records from an internal network.
  - Document Repository Service – Stores documents uploaded by ALUI components.
  - API Service – Provides access to the ALI APIs to enable integration with other ALUI applications, as well as third-party applications.
  - Search Service – Maintains the search collection and processes search requests. Returns indexed content from the resources that are accessible though the portal. These resources can include both ALI resources and resources external to ALI.
- ALI Logger – Provides a logging framework for debugging and diagnostic purposes.
- Support Components
  - Image Service – An area of the local server that stores images and other static content used by the portal and remote services. The Image Service content is non-sensitive data and is stored in a system folder in the local file system. Users of the portal cannot upload content to the Image Service. This component has no role in the TSF of ALI.

The IDK is the external programming interface used for building and implementing user-centric composite applications within the TOE. The IDK provides interfaces for pagelets, portlets and integration web services, such as authentication and profile services, crawlers, and search services.

The TOE depends on the IT environment to provide the file system used by the TOE to protect and store information. Portal information is stored in databases and on disk in the local file system as follows:

- Document Repository – An area of the run-time file system that stores files that are uploaded to the portal.

- Portal database – Tables on a supported database server that store portal administrative data such as object information and security settings.
- Search Server collection – An area of the local server file system that stores indexed ALI document and object data.

6 Documentation

BEA provides an extensive set of documentation describing the installation, configuration, management and operation of the TOE. This set comprises documentation for the ALI and IDK products, which together comprise the AquaLogic Interaction TOE. The AquaLogic Interaction documentation is available from the BEA edocs website, as follows:

- ALI— http://edocs.bea.com/alui/ali/docs61/index.html
- IDK— http://edocs.bea.com/alui/idk/docs60/index.html

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

ALI Guidance

- AquaLogic Interaction Online Help
- BEA AquaLogic Interaction Administrator Guide 6.1 MP1, 14 Dec 2007
- BEA AquaLogic Interaction Installation and Upgrade Guide 6.1 MP1, 17 Sep 2007
- BEA AquaLogic User Interaction Deployment Maintenance Guide, 19 Dec 2007
- BEA AquaLogic User Interaction Networking and Authentication Guide, 19 Dec 2007
- BEA AquaLogic User Interaction Deployment Overview, 19 Dec 2007
- BEA AquaLogic User Interaction Deployment Planning, 19 Dec 2007
- Release Notes for AquaLogic Interaction 6.1

IDK Guidance

- IDK 6.0 Release Notes
- BEA AquaLogic Interaction Development Kit (IDK) Installation Guide, Version 6.0, Dec 2007
- Introduction to Pagelet Development
- IDK QuickStart: Hello World Pagelet (Java | .NET)
- IDK QuickStart: Hello World Portlet (Java | .NET)
- Setting Up a Custom IDK Project (Java | .NET)
- AquaLogic User Interaction Developer Center
- API Documentation (Java | .NET)
- IDK 6.0 API Libraries (Java | .NET)

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 BEA AquaLogic Interaction 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0.

Evaluation team testing was conducted at the vendor's development site November 12 through November 16, 2007.

7.1 Developer Testing

BEA's approach to testing for ALI is based on TOE Security Function (TSF) interface testing. BEA has developed a test suite comprising various automated tests to exercise the TSF at both the user interfaces and the portal and IDK Application Programming Interfaces (APIs) as described in the TOE Functional Specification. These tests were augmented by two (2) manual tests, primarily to support testing of the security audit function. 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 automated test suites and manual tests 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.

While performing the ATE_FUN work units, the evaluation team examined in detail a sample (amounting to slightly over 20%) of the vendor test cases and determined that all actual results matched the expected results. These results provided sufficient confidence that the entire test suite results match as well.

7.2 Evaluation Team Independent Testing

The TOE Test Environment was installed on Microsoft Windows XP Professional and team personnel accessed the following test configurations via virtual machines using VMWare Lab Manager 2.5. The two (2) test configurations selected comprised:

- 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)
- 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

The TOE testing environments were equipped with the following software:

- AquaLogic Interaction 6.1 MP1
- AquaLogic Interaction Development Kit 6.0
- Microsoft Active Directory 6.3

- Sun Java 2 SDK 1.4.2_11 with Java HotSpot™ Client VM
- Microsoft Internet Explorer (IE) 6.0 SP2.

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

The evaluation team performed the following additional functional tests:

- **Auditing of invalid login attempts**—the vendor's Strength of Function (SOF) analysis states, in part, that invalid login attempts are audited. As described in the AVA_SOF work units, the evaluation team was unable to find supporting evidence for this claim in the ST or design documentation. The team demonstrated that invalid login attempts are not audited. The vendor was required to revise the SOF analysis accordingly.
- **Confirmation of audit record content**—the vendor's Test Documentation did not identify any checks that generated audit records contain at least the information specified in FAU_GEN_EX.1.2, or that every auditable event is associated with the identity of the user that caused the event (FAU_GEN.2). The test demonstrated that each auditable event specified in the functional specification is captured in the audit records and satisfies the requirements specified in the ST.
- **Default Access Control List (ACL) validation**—Section 6.1.2 of the ST identifies the initial default ACLs associated with the folders that are created when the TOE is installed. It was not clear that the vendor's testing adequately demonstrated these defaults are in place when the TOE is installed. The test found that default users and groups did not match the ST, nor did the default folders in the Administrative Objects Directory match the ST. Further, the default user, group or profile access privileges and activity rights were incorrect. The test resulted in updates to the ST to correct the discrepancy.
- **Minimum password length—**as reported in the AVA ETR, the vendor's SOF analysis based its calculations partly on the claim that passwords have a minimum length of five (5) characters. The test demonstrated that a user may not enter a password of less than five (5) characters.
- **Password alphabet**—as reported in the AVA ETR, the vendor's SOF analysis based its calculations partly on the claim that the available password alphabet comprises 94 characters. The test demonstrated that all 94 printable characters of the standard typewriter keyboard can be used in the password.
- **Default account lockout configuration**—as reported in the AVA ETR, the vendor's SOF analysis claims that by default the TOE is configured with User Lockout enabled, although the default values for controlling this feature (lockout after 20 failed attempts within 10 minutes, for a one (1) minute period) need to be modified in order to meet SOF-Basic. The test demonstrated that an administrator can change the Account Lockout default values, such that the new values take effect.
- **Authentication failure parameters**—the specification of FIA_AFL.1 indicated the administrator could set the number of failed portal login attempts allowed before the user account is locked to a number between 1 and 100. It was unclear if this restriction was enforced by the TSF, or what would happen if an Administrator attempted to specify a

number outside this range (e.g., 0, 101). The test demonstrated that: a) there is no upper limit on the range that can be configured; b) zero (0) behaves the same as one (1); and, c) the account is not locked until the configured number is surpassed (e.g., the recommended setting of five (5) does not lock out the user account until after six (6) unsuccessful attempts). The test resulted in changes to the ST and the SOF analysis.

- **Authentication failure behavior**—the statement of FIA_AFL.1 specified the behavior of the TSF as follows: "When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall…" The TSS stated that the TOE locks out user accounts when the administrator-configured unsuccessful login attempts threshold is reached (i.e., when the defined number of unsuccessful authentication attempts has been met). It was not clear from either the vendor tests or some of the evaluation team tests that this was in fact the behavior of the TOE. The test demonstrated the TOE locks user accounts only after the unsuccessful authentication attempts value is surpassed, not when it is met. The TSS in the ST was updated to correctly describe the behavior of the authentication failure handling mechanism. In addition, this behavior affected the vendor's SOF analysis, which assumed the user account is locked when the failed attempts threshold is met. Since the account is not locked until the threshold is surpassed, this increased the number of passwords that could be guessed by an attacker in a given time period (i.e., 6 per hour, or 144 per day). The SOF analysis was recalculated based on this behavior and showed that the password authentication mechanism still achieves SOF-Basic.

- **Authentication failure window**—the description of the authentication failure handling mechanism in the ST stated that the TOE keeps track of the configured number of failed login attempts in a configured time period ("Minutes to track failed logins"). The description of the security management function for managing these values indicated the number represents the number of consecutive failed logins, but it was not clear this is the case. The test demonstrated the authentication failure mechanism behaves as follows: failed login attempts do not need to be consecutive in order to lock the user account; the act of unlocking a locked user account sets the failed login count to 0; the TOE tracks the number of failed login attempts within the last *x* minutes from the current failed attempt (rather than resetting the count every *x* minutes). In summary, the TOE, each time a login attempt fails, counts the number of failed attempts in the last *x* minutes, or since the account was last unlocked, whichever is most recent.

- **Enforcement of external identification and authentication**—the ST specifies that the TSF requires users whose accounts are defined in the IT environment to be successfully identified and authenticated by mechanisms in the IT environment before being allowed to access the TOE (FIA_ENF_EX.1). The developer specified positive tests of this capability, but it was unclear if any negative tests are included in the developer's test suite. The test demonstrated the TOE enforces the external authentication decision. As a side note, during conduct of this test, the evaluator entered the username "test&user" (NOT "test&user1") without a password and was surprised to find the user was logged in. Investigation identified that the userid "test&user" also existed in the Active Directory repository, without a password specified for the account. This was also demonstrated by attempting, unsuccessfully, to logon as "test&user" with a password of "plumtree".

- **Enforcement of authentication failure handing at API**—the functional specification describes the getExplicitLoginContext method of the IRemoteSession interface, which is

part of the Programmable Remote Client (PRC) API. This method is used to establish a session with the TOE through the API and requires the specification of a user name and password. However, it is unclear from the functional specification if this interface enforces authentication failure handling, in the case where an application attempts to guess a user's password. The test demonstrated that authentication failure handling is enforced at the API.

- **Restrictions on ACL management**—the ST specifies that the capability to modify object ACLs is restricted to administrators and users with the Admin privilege on the object. The vendor's tests demonstrate that administrators can modify ACLs, but it is unclear that the specified restrictions are tested. The test demonstrated that the TOE restricts the ability to modify the ACL on an object to the Administrator and to users with Admin access to the object.
- **Restrictions on group management**—the ST specifies that the capability to assign activity rights to groups is restricted to administrators. The vendor's tests demonstrate that administrators can assign activity rights to groups, but it is unclear that the specified restrictions are tested. The test demonstrated that non-administrative users are unable to manage activity rights on groups.
- **Overriding default ACL on object creation**—the ST specifies that the capability to specify an alternative initial ACL to override the default ACL when an object is created is restricted to administrators and users with the Admin privilege on the parent object. It is unclear that the vendor's tests demonstrate this capability, or the restrictions. The test demonstrated that the TSF restricts the ability to specify an initial ACL to the administrator and a user with Admin privilege on the parent object.
- **Management of user accounts**—the ST specifies that the capability to manage most of the user security attributes and user accounts is restricted to the administrator. It is unclear that the vendor's tests demonstrate this restriction. The test demonstrated that the TOE enforces the restriction on management of user accounts to administrators.
- **Management of authentication failure parameters**—the ST specifies that the capability to manage the values that control the authentication failure handling capability is restricted to the administrator. It is unclear that the vendor's tests demonstrate this restriction. The test demonstrated that only members of the administrator's group can manage the values that control authentication failure handling.
- **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. These tests were supported by additional tests that showed that users must be identified and authenticated before they can get access to the TOE (with the exception of Guest users, that have no access permissions except those available via the Everyone group). The evaluation team's tests demonstrated that restrictions on security management capabilities are enforced and that authentication failure handling is performed through both the GUI and the API. The evaluation teams' penetration 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:

- **User account locking vulnerability**—testing of other BEA products in other evaluations identified a vulnerability in User Account Locking, whereby more than the configured number of invalid login attempts could be made because the lockout functionality treated user ids as case sensitive, but the authentication function did not (i.e., the authentication function treated "User" and "user" as the same user identity, but the lockout function kept separate counts of failed login attempts for these two identities, resulting in an attacker being able to make more password guesses against a target user identity than should have been allowed). The test demonstrated the expected behavior—usernames are not case sensitive and are not treated as such by the authentication failure mechanism.
- **ALI Login Page 'Remember my password'**—the ALI Login Page contains a checkbox where a user can check to 'Remember my password.' The evaluators were concerned that this would allow a user in the Administrators Group to check this box and that while away from the machine, an unauthorized user could attempt to gain entry by guessing the user ID (commonly administrator) and without entering a password, gain entry. The test demonstrated that although a new user was created within ALI as a member of the Administrators Group, users must enter a password at the login screen in order to access the TOE, regardless if the Remember my password box is checked.
- **Navigate to unauthorized functions**—the authorized administrators access the TOE via a web-based interface. The purpose of this test is to enter in 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 demonstrated that the TOE performs checks that the user has sufficient permissions to view a portal page or access capabilities provided by that page. Although the URLs that were used were ones that were generated by an administrative user, the TOE does not rely on parameters in the URL to determine the user identity. If the user is not logged in and attempts to edit a portal object, the TOE will log the user in as the Guest user and provide access based on the permissions of the Guest user and Everyone group (of which Guest is a member). If the user is not logged in and attempts to access a system utility, the TOE requests the user to login first, then determines if the logged in user has appropriate permissions to access the system utility. For example, the user must be a member of the Administrators group in order to access the Portal Settings system utility.
- **PHP remote file inclusion**—the technology type of the TOE is potentially vulnerable to PHP remote file inclusion attacks. The evaluation team explored the TOE's susceptibility to this form of attack. The evaluation team checked the TOE installed files and did not identify any that appeared to be implemented in PHP. The evaluation team did not identify any scope for attempting this type of attack at the TSFI.

7.4 Post-Testing Activities

Subsequent to the evaluation team testing activities, but prior to the formal conclusion of the evaluation, the vendor posted four security advisories relevant to the TOE on its Security Advisories and Notifications web page (http://dev2dev.bea.com/advisoriesnotifications/). These are summarized as follows:

- BEA07-179.00: BEA Plumtree Foundation[2] internal hostname disclosure vulnerability—this vulnerability is addressed by configuration changes described in the text of the security advisory
- BEA07-180.00: BEA Plumtree Foundation full version vulnerability—this vulnerability is addressed by configuration changes described in the text of the security advisory
- BEA07-181.00: BEA Plumtree Foundation search facility allows an unauthenticated guest user to search for user objects—this vulnerability is addressed by configuration changes in the text of the security advisory
- BEA08-186.00: BEA Plumtree Portal cross site scripting (XSS) vulnerability—this vulnerability is addressed by applying the patch provided with the security advisory, which brings the ALI portion of the TOE into its evaluated configuration (AquaLogic Interaction 6.1 MP1 Patch 2).

8 Evaluated Configuration

The evaluated version of the TOE is AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0.

The TOE is a portal technology platform (ALI) and its associated development kit (IDK). Some of the ALI components run on application servers and other components run as Windows services or UNIX daemon processes (depending on the operating system platform). The IDK typically runs on a separate remote server from ALI and has its own IT requirements. Tables 2-1 and 2-2 in the ST list the IT environment components for ALI and IDK respectively.

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

[2] ‘Plumtree Foundation’ and ‘Plumtree Portal’ are previous product names for AquaLogic Interaction.

for BEA AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0.

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

Patch 2 was developed by the vendor after the independent testing performed by the CCTL. The Validators reviewed the changes applied by Patch 2 and determined that the changes were well below the scope of the evaluation's level of examination and approved it for inclusion in the evaluated configuration without requiring retesting. This is in conformance with established assurance maintenance procedures, except that the assurance maintenance occurred while finalizing the initial evaluation.

Configuring the product to use SSL is an optional step in the configuration process, but the Validators highly recommend that it be done to mitigate the possibility of a replay attack on the process of authenticating users to remote portlets.

It should be noted that administrators can be locked out of the system for a period of time by an attacker who invokes several failed authentication attempts. Giving administrators user names that are difficult to guess would mitigate this threat.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **AquaLogic® Interaction 6.1 MP1 Patch 2 with AquaLogic® Interaction Development Kit 6.0 Security Target,** Version 1.0, dated 23 April 2008.

13 Glossary

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

- **J2EE**—Java2 Platform, Enterprise Edition
- **JDK**—Java Development Kit
- **LDAP**—Lightweight Directory Access Protocol
- **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:

- *BEA AquaLogic Interaction 6.1 MP1 Patch 2 with AquaLogic Interaction Development Kit 6.0 Security Target*, Version 1.0, 23 April 2008.