National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

IBM

WebSphere Application Server V7.0.0.19 (32-bit) with interim fix for APAR PM53930

Report Number: CCEVS-VR-VID10442-2012
Dated: 25 May 2012
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel P. Faigin
The Aerospace Corporation
El Segundo, California

Franklin Haskell
The Mitre Corporation
Bedford, MA

John Nilles
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Dawn Campbell
Eve Pierre
Chris Keenan
SAIC
Columbia, MD

Table of Contents

List of Figures

List of Tables

1 EXECUTIVE SUMMARY

The Target of Evaluation (TOE) is the WebSphere Application Server V7.0.0.19 (32-bit) with interim fix for Authorized Program Analysis Report (APAR) PM53930. The evaluation of the TOE was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in May 2012. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 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 TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4 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.

The TOE is IBM's implementation of an application server, which is compliant with Java EE 5 specification. The primary purpose of the product is to provide an environment for running and managing user-supplied enterprise applications and their components. In particular, the product provides the capabilities to identify users and to control what resources a user can access through enterprise applications. In addition to its primary purpose, the product provides tools for doing useful functions such as assembling and troubleshooting enterprise applications.

The product, when configured as specified in "WebSphere Application Server EAL4 AGD – Guidance", satisfies all of the security functional requirements stated in the IBM WebSphere Application Server v7.0.0.19 (32-bit) with APAR PM53930 EAL4+ Security Target (ST).

2 IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation granted by the National Institute of Standards and Technology (NIST).

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 (PP) to which the product is conformant;
- The organizations and individuals participating in the evaluation.

Table 1. Evaluation Identifiers

Evaluated Product:	WebSphere Application Server V7.0.0.19 (32-bit) with interim fix for APAR PM53930
Sponsor:	IBM, Inc. 11501 Burnet Road Austin, Texas 78758
Developer:	IBM, Inc. 11501 Burnet Road Austin, Texas 78758
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	10 October 2010
Completion Date:	25 May 2012
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	EAL 4 augmented with ALC_FLR.2

Description:	The product is IBM's implementation of an application server, which is compliant with Java EE 5 specification. The primary purpose of the product is to provide an environment for running and managing user-supplied enterprise applications and their components. In particular, the product provides the capabilities to identify users and to control what resources a user can access through enterprise applications. In addition to its primary purpose, the product provides tools for doing useful functions such as assembling and troubleshooting enterprise applications.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the IBM WebSphere Application Server products by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Dawn Campbell Eve Pierre Chris Keenan
Validation Body:	National Information Assurance Partnership CCEVS

2.1 Interpretations

Not applicable.

3 SCOPE OF EVALUATION

3.1 Threats

The ST identifies the following threats that the TOE and its operating environment are intended to counter:

- A caller gains access to a resource without the correct authority to access that resource.
- An unidentified caller gains access to a protected resource.
- Data transferred between workstations is disclosed to, or modified by unidentified users or processes, either directly or indirectly.
- The misconfiguration, inappropriate installation, or inappropriate development of applications and operating system that the TOE interfaces with, compromises the TOE security policies or security functions used to protect sensitive resources from access by unauthorized remote[1] callers.

[1] A remote caller is a user from a remote JVM

3.2 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operating environment are intended to fulfill:

- The right to access a resource is determined on the basis of association of user or group IDs to roles and of roles to resources.

This organizational security policy essentially implements the AC-3 (Access Enforcement) control defined in NIST SP 800-53 Revision 3: "the information system enforces approved authorizations for logical access to the system in accordance with applicable policy". In particular, it implements AC-3(3) when used with the Role Based Access Control (RBAC) and access control policies as defined in Section 3.3 of this document.

3.3 Physical Scope

The Target of Evaluation is:

- WebSphere Application Server V7.0.0.19 (32-bit) with the interim fix for APAR PM53930.

The TOE consists of the following components, which are described in Section 6:

- Product Application Server
- Product Hypertext Transfer Protocol (HTTP) Server
- Product HTTP Server Plug-Ins
- Product *wsadmin* Tool

The TOE has been designed to control access to the data it hosts and the associated management functions. This is accomplished by offering access to its objects and functions through interfaces carefully designed to ensure that the applicable security policies are enforced prior to allowing requested operations to succeed. However, the TOE is an application program that depends on the supporting products identified above and summarized below. As such, the TOE is dependent upon those products to enforce their respective policies to ultimately protect the TOE and its data both at rest and while in execution.

The following software components are not included in the TOE. They are part of the TOE operational environment in the evaluated configuration:

- *Operating system*. The evaluated configuration of the TOE is supported on the following operating systems:
    - AIX® 6.1 (64-bit);
    - HP-UX 11i v2 (64-bit PA-RISC);
    - Linux® Redhat 5.1 on PPC (64-bit) / Intel™ / System z®;
    - Linux SuSE Enterprise Edition 10 (SLES 10) on PPC (64-bit) / System z;
    - Oracle Solaris 10 (64-bit);

- Microsoft® Windows® Server 2008;

It is assumed that all hardware used within the operating environment is secured such that no potential vulnerabilities could be introduced that would circumvent the functionality described within this ST. This protection is assumed to be both physical and logical (for example, appropriate use of network boundary protection devices).

- *Product Java 2 Software Development Kit (SDK)*. The SDK used by the evaluated configuration is:
  - *On HP-UX:* HP Java Development Kit (JDK) for Java 2 Platform Standard Edition (J2SE) HP-UX 11i platform, adapted by IBM for IBM Software, Version 6.0
  - *On Oracle Solaris:* IBM SDK for Solaris, Java 2 Technology Edition, Version 6.0
  - *On all other platforms*: the IBM SDK for multiplatforms, Java Technology Edition, V6.0
- *Java Database Connectivity (JDBC) resource and any back-end servers*. The TOE was evaluated with the following JDBC provider, as well as the back-end server used by this provider: IBM DB2® v8.2. The provider was configured to run inside the Product Application Server component of the TOE and to access data stored in the back-end server.
- *Lightweight Directory Access Protocol (LDAP) server*. The TOE was evaluated with the following LDAP server, which was configured as the user registry: IBM Tivoli® Directory Server 6.2.
- *IBM Cryptography for C*. The TOE was evaluated with IBM Cryptography for C as the cryptographic service provider. IBM Cryptography for C is a FIPS 140-2 validated cryptographic module. The cryptographic module is provided by the operational environment through IBM Global Security Kit (GSKitv7), which has been separately evaluated.

Note that the TOE must be configured in accordance with the set of evaluated Guidance documentation—in particular, the "WebSphere Application Server EAL4 AGD – Guidance" document—which can be downloaded from http://www.ibm.com/support/docview.wss?uid=swg24030364. This documentation includes

- The Installation and Configuration Guide for the Certified System,
- Administrator's Guide for the Certified System,
- Developers Guide for the Certified System.

The Guidance documentation includes links to pertinent on-line documents in the WAS Information Center at http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/welcome_base.html. The web pages at the Information Center link also include product information and operating environment information not necessarily specific to the TOE, which have not been evaluated, and

should be considered for informational purposes only as they may contain instructions not suitable for use in the evaluated configuration. Only the Guidance documents identified above and the links to web pages within the Installation and Configuration, Administrator, and Developer's Guides should be considered as specific guidance for the TOE.

3.4 Logical Scope

The description of the security features of the product are described in further details in Section 4. In summary, these functions are:

- Security Audit
- Identification
- Access Control
- Security Management
- Invocation of Secure Socket Layer (SSL)

3.5 Excluded Features

The Product Tools and Applications component has capabilities for product upgrading and migration. These capabilities are not applicable in the evaluated configuration and were excluded from evaluation.

The following product components are excluded from evaluation:

- Proxy Server
- Admin Console
- Admin Agent
- Job Manager

These components are not configured as part the TOE.

Refer to the User Guidance document for specific configuration requirements.

Product features that are not identified as part of the TOE and that are not explicitly excluded are available in the evaluated configuration but were not covered by the evaluation. These features do not contribute to meeting the security functional requirements claimed for the TOE.

4 SECURITY POLICY

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

> ***Note:*** *Much of the description of the WebSphere Application Server security policy has been extracted and reworked from the WebSphere Application Server ST and Final ETR.*

4.1 Security Audit

The TOE provides an auditing mechanism for auditing identification and access control events. The TOE provides the capability to enable and disable auditing; and for reviewing the audit records to authorized administrators. The audit functions are able to associate users with security relevant actions for identification, access control and for enabling and disabling the audit function. The TOE relies on the operational environment for audit record storage.

4.2 Identification

The TOE provides functions that identify a remote caller when the caller requests access to a sensitive resource protected by the TOE. These functions are:[2]

- Ident.1—This function identifies a remote caller that requests access to a sensitive resource using a remote HTTP/S Interface of the TOE.
- Ident.2—This function identifies a remote caller that requests access to a sensitive resource using a remote Object Request Broker (ORB) interface of the TOE.
- Ident.3—This function identifies a remote caller that requests access to a sensitive resource using a remote Java Message Service (JMS) interface of the TOE.
- Ident.4—This function re-identifies a remote caller that requests access to a sensitive resource using a remote web services interface of the TOE. The TOE does initial identification base on initiating request through Ident.1.
- Ident.6—This function permits a method in a deployed user web server application or enterprise bean to assume the identity of another user.
- Ident.7—This function identifies a remote caller when the remote caller attempts to access a sensitive transaction using the remote Web Services Transactions (WS-Transactions) interface of the TOE.

For authentication, the TOE accepts the user information (user ID/password, token, or certificate) and passes that information to the operational environment. The operational environment determines if the information is valid and returns that status to the TOE. If the information was valid the TOE creates a Subject that contains a credential with the user information. The TOE uses the Subject for subsequent identification and authorization checks. If the operational environment determines the identification information is not valid, then the TOE does not create a Subject and instead throws a login failure exception.

The TOE relies on the operational environment and on the user IDs and group IDs maintained by the environment to authenticate claimed identities when TOE policy requires authentication.

[2] Note: Function Ident.5 is not applicable in this configuration of the product. The function is applicable to the sibling products, “WebSphere Application Server Network Deployment v7.0.0.19 (32-bit) with APAR PM53930” and “WebSphere Application Server for z/OS V7 Service level 7.0.0.19 with APAR PM55522”.

4.3 Access Control

The TOE provides access control functions that allow only authorized remote callers to access to the sensitive resources. A sensitive resource is defined as a resource that:

- Resides in a server TOE component
- Can be accessed by a remote caller, which is an entity residing outside the server TOE component in which the sensitive resource resides.
- Could be used by a remote caller to compromise the security of a deployed web server application or deployed enterprise bean.

The following are the sensitive resources of the TOE:

- Methods and static web content of deployed user web server applications (user web server applications that are deployed in the TOE)
- Methods of deployed user enterprise beans (user enterprise beans that are deployed in the TOE)
- Transactions and activities of deployed user web server applications, deployed enterprise beans, and the TOE
- The TOE naming directory
- The TOE Universal Description Discovery and Integration (UDDI) registry directory
- TOE configuration data
- TOE runtime state
- TOE local bus, queue destinations, temporary destinations, topic space, topic space root, and topics

The following are the access control functions:[3]

- AC.1—This function controls access from remote callers to methods and HTML pages in deployed web server applications.
- AC.2—This function controls access from remote callers to Methods in deployed enterprise beans (including methods that are deployed as web services endpoints).
- AC.3—This function controls access from remote callers to TOE configuration data, and TOE runtime state.
- AC.4—This function controls access from remote callers to the TOE naming directory.
- AC.5—This function controls access from remote callers to transactions and activities.

[3] Note: Function AC.8 is not applicable in this configuration of the product. The function is applicable to the sibling product, "WebSphere Application Server Network Deployment v7.0.0.19 (32-bit) with APAR PM53930".

- AC.6—This function controls access from remote callers to messaging resources (local bus, queue destinations, temporary destinations, topic space, topic space root, and topics).
- AC.7—This function controls access from remote callers to UDDI resources.
- AC.9—This function controls access from remote callers to methods and attributes in user MBeans.

The TOE bases access control decisions on identity and roles of the remote caller and permissions required for the target resource. The TOE relies on the operational environment and on the user IDs and group IDs maintained by the environment to authenticate identity. Each resource's configuration determines the permissions required to access the resource. Permissions are defined for applications and deployed together. Once deployed, these permissions can only be changed by a user with an ID mapped to an Administrator role, Configurator administrator role, or for application data only, the Deployer role.

The TOE builds an authorization table based on information from the applications for Enterprise Java Beans (EJBs) and web resources, and admin policy files for the Application Server. Upon a request the TOE will use the credential from the Subject making the request and determine if the corresponding user (or group the user belongs to) is in the role definition required for that resource. If the user/group is in the required role, then the TOE grants access; otherwise, the TOE denies access.

4.4 Security Management

The TOE provides security management functions that provide a mechanism for dynamically configuring some security attributes used by TOE access control functions

4.4.1 Administration Roles

The TOE maintains the following Administration roles:

- Administrator
- Configurator
- Monitor
- Operator
- Deployer
- AdminSecurityManager
- Auditor

These roles may be used to perform operations on objects as indicated in Table 2.

Table 2. Management Capabilities of Administration Roles

Role	Objects	Operations
Administrator Configurator Monitor Operator Deployer (configuration data for applications only)	TOE configuration data	Read
Administrator Configurator Deployer (configuration data for applications only)	TOE configuration data	Modify *Note: This applies to all attributes except the attributes that map user/group IDs to administration roles.* *Note: This includes the attributes listed in SM 1.4 except for the runtime attribute that stores the list of registered UDDI publishers.*
AdminSecurityManager	TOE configuration data	Modify attributes that map user/group IDs to administration roles.
Administrator Configurator Monitor Operator Deployer (application runtime state only)	TOE runtime state	Read
Administrator Operator Deployer (application runtime state only)	TOE runtime state	Modify *Note: this includes the runtime attribute that stores the list of registered UDDI publishers.*
Administrator	Transactions and activities Naming directory Messaging Registered UDDI Publishers	All operations Modify attributes that map user/group IDs to Naming roles Modify attributes that map user/group IDs to Messaging roles Modify or delete attributes

Role	Objects	Operations
Configurator	Naming directory Messaging	Modify attributes that map user/group IDs to Naming roles Modify attributes that map user/group IDs to Messaging roles
Operator	Registered UDDI Publishers	Modify or delete attributes
Monitor	Naming directory	view
Auditor[4]	Security audit function	Disable and enable
AdminSecurityManager	Security audit function The attributes that map user/group IDs to administration roles	Disable and enable All operations
One or more Administration roles	Protected methods in user MBeans	invoke
One or more Administration roles	Protected attributes in user MBeans	read
One or more Administration roles	Protected attributes in user MBeans	write

4.4.2 Naming Roles

The TOE maintains the following Naming roles:

- COSNamingCreate
- COSNamingDelete
- COSNamingRead
- COSNamingWrite

These roles may be used to perform operations on objects as indicated in Table 3.

[4] Enable and disable of the security audit function is audited.

Table 3. Management Capabilities of Naming Roles

Role	Objects	Operations
COSNamingDelete	TOE naming directory	Delete access
COSNamingDelete COSNamingCreate	TOE naming directory	Create access
COSNamingDelete COSNamingCreate COSNamingRead COSNamingWrite	TOE naming directory	Read access
COSNamingDelete COSNamingCreate COSNamingWrite	TOE naming directory	Write access

4.4.3 Universal Description Discovery and Integration (UDDI) Roles

The TOE maintains the following UDDI roles:

- SOAP_Publish_User
- V3SOAP_CustodyTransfer_User_Role
- V3SOAP_Publish_User_Role
- V3SOAP_Security_User_Role
- EJB_Publish_Role

These roles may be used to perform operations on objects as indicated in Table 4.

Table 4. Management Capabilities of UDDI Roles

Role	Objects	Operations
SOAP_Publish_User or *V3SOAP_Publish_User_ Role*, and List of registered UDDI Publishers	Protected UDDI registry resources through the HTTP interface	All operations on the Simple Object Access Protocol (SOAP) V1, V2 and V3 Publish API
V3SOAP_ CustodyTransfer_User_ Role, and List of registered UDDI	Protected UDDI registry resources through the HTTP interface	All operations on the SOAP V3 Custody Transfer API
V3SOAP_Security_User_ Role List of registered UDDI Publishers	Protected UDDI registry resources through the HTTP interface	All operations on the SOAP V3 Security API
EJB_Publish_Role	Protected UDDI registry resources through the ORB interface	All operations on the V2 Publish API

4.4.4 Messaging Roles

The TOE maintains the following Messaging roles:

- Browser
- Bus Connector
- Creator
- Receiver
- Sender

The Bus Connector roles (Messaging) have their own administrative commands that are restricted to viewing and managing the users associated with the Bus Connector and default bus roles. These roles may be used to perform operations on objects as indicated in Table 5.

Table 5. Management Capabilities of Messaging Roles

Role	Objects	Operations
Bus connector	Local Bus	Connect to the local bus for messaging services.
Creator	Queue destination	Create a queue destination.
Sender	Queue destination	Send a message to a queue destination.
Receiver		Receive a message from a queue destination.
Browser		Browse messages within a queue destination.
Creator	Temporary destination	Create a temporary destination.
Sender		Send a message to a temporary destination.
Receiver		Receive a message from a temporary destination.
Browser		Browse messages within a temporary destination.
Sender	Topic Space	Send a message to a topic space
Receiver		Receive a message from a topic space
Sender	Topic Space Root	Send a message to a topic space root
Receiver		Receive a message from a topic space root
Sender	Topics	Send a message to a topic
Receiver		Receive a message from a topic

4.5 Invocation of Secure Socket Layer (SSL)

The TOE provides an invocation of SSL function that requires a remote caller to invoke TLS 1.0 using the configured algorithms so that the session is encrypted when the remote caller issues a request to the TOE over the remote interface of the IBM HTTP Server component. This function does not perform the actual SSL encryption, yet provides a mechanism for requiring requests from remote callers to be encrypted.

The cryptographic operation and support requirements are provided by the operational environment. The algorithms used are implemented in a FIPS validated cryptographic module.

5 CLARIFICATION OF SCOPE

5.1 Assumptions

The ST identifies the following assumptions about the use of the product:

1. It is assumed that the operational environment supporting the TOE provides at least one of the supported authentication mechanisms identified within the evaluated configuration of the TOE.
2. It is assumed that the applications and operating system that the TOE interfaces, will not compromise the security of the TOE and where applicable, that they have been configured in accordance with manufacturer's installation guides and/or its evaluated configuration. It also is assumed that the developers of all user applications (user web server applications and user enterprise beans), resource adapters, and providers will comply with all the guidelines and restrictions specified in the User Guidance document.
3. It is assumed that the operational environment provides accurate timestamp information.
4. It is assumed that the operational environment supporting the TOE provides the means to store, protect, and access data within files.
5. It is assumed that all software and hardware, including network and peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data. It is assumed that all hardware used in the operating environment is secured.
6. 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, wilfully negligent or hostile. It also is assumed that this individual will comply with all the guidelines specified in the User Guidance document.

5.2 Limitations and Exclusions

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 augmented with ALC_FLR.2).
2. This evaluation only covers the specific edition and software version identified in this document, and not any earlier or later versions released or in process.
3. The following product components are excluded from evaluation: Proxy Server, Admin Console, Admin Agent, and Job Manager.
4. The TOE utilizes third-party software and hardware components in its operational environment, as follows:
    a. Operating System
    b. Java 2 SDK - provides a Java execution environment (Java Virtual Machine (JVM)) for the rest of the TOE.
    c. JDBC resource and back-end servers - The UDDI and Built-in JMS Resource services of the TOE use the provider and back-end server to store UDDI and messaging data.
    d. LDAP Server – provides the user registry.
    e. IBM Cryptography for C – used for secure communication support.
5. The Operating System and the JVM must be regularly patched and maintained to ensure a secure operating environment for the TOE. The IBM JDK support policy for fix packs[5] is located at http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg21138332. Based on this policy, The IBM WebSphere Application Server Java SDK can be upgraded to the latest service release for the same Java SDK version. Customers should download the latest version of the 1.6 JDK to ensure a secure safe operating environment.
6. Applications that the TOE hosts are not covered in the evaluation. The application developers are assumed to follow guidance for a certified system in User Guidance and that administrators deploy only those applications. Consequently, some types of applications, services, and Web Services must not be used in the evaluated configuration.

    The following types of applications must not be deployed in the evaluated configuration:

[5] A "fix pack" is a cumulative collection of Authorized Program Analysis Reports (APAR) fixes. They are intended to allow the user to move up to a specific maintenance level. They have the following characteristics:

- They are cumulative.
- They are available for all supported operating systems.
- They contain many APARs.
- They are published on the IBM Support Portal.
- They are fully tested by IBM.
- They are available only in English.

a. Applications provided with WebSphere Application Server, except for the UDDI Registry Application
b. Session Initiation Protocol (SIP) applications
c. Portlet applications
d. Applications using request dispatching

The following types of services must not be used in the evaluated configuration:

a. Activity session service
b. Data Replication service
c. Compensation Scoping Service
d. Event service
e. WS-Notification services

The following types of web services must not be used in the evaluated configuration:

a. Web Services Gateway
b. Web service endpoints using JMS transport (only HTTP is in the evaluated configuration)
c. Web Services JAX-WS applications (see Web Services above)
d. JAX-RPC web services using Kerberos (see Web Services above)

6 ARCHITECTURAL INFORMATION

This section provides a high level description of the TOE and its components as described in the Security Target and design documentation.

The WebSphere Application Server TOE consists of a subset of the components provided with the product. This subset is comprised of those product components that are used to deploy and run user-supplied enterprise applications and to manage these applications by means of a scripting tool.

Specifically, the WebSphere Application Server TOE consists of the following WebSphere Application Server product components: Product Application Server, Product HTTP Server, Product HTTP Server Plug-Ins, Product Tools and Applications, Product Deployment Manager Server, and Product Node Agent Server.

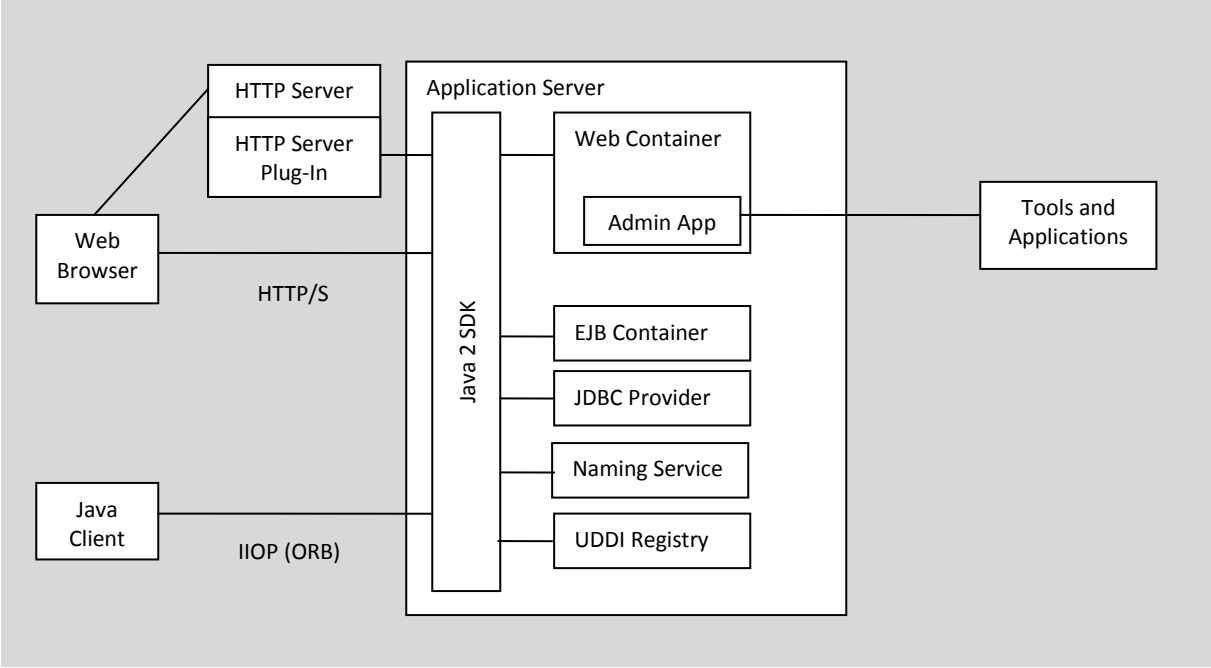

Figure 1. Product Overview

6.1 Product Application Server

The Product Application Server component is a set of containers, services, and resources that provides an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components. This environment separates application logic from infrastructure. The enterprise application developer implements applications (for example, an EJB to containing business logic to access a legacy database). The Product Application Server implements infrastructure (for example, a container for the EJB) so that each application need only implement business logic. The infrastructure provides communication and security functions, which include, for example, user identification and authorization. It provides centralized mechanisms to deploy and manage enterprise applications within the infrastructure. Moreover, the physical and logical measures in the environment that protect the Product Application Server likewise protect the enterprise applications that reside with the server.

The containers are runtime wrappers that handle system functions, such as communications and security, for enterprise application components and some types of resources. The following containers are included:

- **Enterprise bean container**—handles system functions for enterprise beans.
- **Web server container** (contains an embedded HTTP server)—handles system functions for web server applications.
- **Resource adapter container**—handles system functions for resources that conform to the Java 2 Platform Extended Edition (J2EE) Connector Architecture (JCA).

The services are Java API and remote interface implementations. They provide useful functions, such as directory and security that components of enterprise applications can use. A few of these services also are remotely available so that Java clients also can use them. The following services are included:

- **Services defined and documented in Java specifications**. These services are identified in the formal product documentation.
- **Additional, product-specific services**, which are also defined and documented in the formal product documentation.

The resources are software modules that are used by some of the services for back-end processing. The following resources are included:

- **A built-in Java Database Connectivity (JDBC) provider**, which is sometimes referred to as the "WebSphere Relational Resource Adapter"—handles back-end processing for the product JDBC API service and uses its own built-in database server for storing and retrieving storage.
- **A built-in Java Message Service (JMS) Provider**, which is sometimes referred to as the "Default Messaging Provider"—handles back-end processing for the product messaging service.
- **A naming resource**—handles back-end processing for the product Java Naming and Directory Interface (JNDI) and COSNaming services.
- **The UDDI Registry Application**, which provides a directory for storing web services endpoints.
- **Security resources**—handles back-end processing for the product security services using a user registry in the environment.

In this evaluation, it has been tested that when the TOE is in its evaluated configuration, the Product Application Server protects each remotely accessible resource through security checks for identification and access control.

In the evaluated configuration, the Product Application Server performs the following functions:

- **Starts up**. The Product Application Server is started using the Java command provided by the Product Java 2 SDK. The Product Application Server is run in a single operating system process and JVM.
- **Loads local components**. The Product Application Server starts the following components: User applications (that is, web server applications and enterprise beans), and UDDI Registry Application. Note that the Application Server loads policy definitions from the deployment descriptors which provide access control definitions for the applications. The local components run in the same operating system process and JVM that the Product Application Server is using. Therefore, these components are called "local components."

  For user applications, the TOE supports Enterprise JavaBean specifications 2.1 and lower. It supports Java Servlet specification 2.4 and lower.

- **Accepts local and remote requests**. The Product Application Server accepts requests over its local and remote interfaces. The requests over its local interfaces come from the local components (web server applications and enterprise beans). The Product Application Server receives these requests directly. The requests over its remote interfaces come from Java clients. The Product Application Server receives these requests indirectly by means of the Product Java 2 SDK.

- **Processes requests for services**. If the Product Application Server receives a request for a service, the Product Application Server first performs any actions required by the security configuration (for example, identification and access control). If actions are successful, the Product Application Server processes the requested service. In the evaluated configuration, the Product Application Server enforces the security checks for the following services: Administration service; Naming service; Messaging service (when the Product Application Server is configured to use the Built-In JMS Provider); and UDDI Service.

- **Processes requests for mapped methods and HTML pages.** If the Product Application Server receives a request for a mapped method or HTML page in a user application or the UDDI Registry Application, the Product Application Server first performs any actions required by the security configuration (for example, identification and access control). If the actions are successful, the Product Application server invokes the mapped method or HTML page.

- **Web Services.** The product supports two types of Web Services applications – JAX-WS and JAX-RPC. However, the evaluated configuration of the product includes only the support for JAX-RPC. As such, while the product includes a number of web services support features, specifically WS-ReliableMessaging, WS-SecureConversion, WS-Security, and WS-Kerberos, those features are excluded due their reliance on JAX-WS. The support for JAX-WS and these other specific features is excluded from the evaluated configuration due to very limited use by customers, reliance on external security products (e.g., a KDC), and some inherent limitations or conflicts among the available supporting functions.

Multiple instances of the Product Application Server can be configured on the network and in a single operating system. Each instance of the Product Application Server runs in its own process and JVM.

6.1.1 Required configuration of the Product Application Server

In the evaluated configuration, the Product Application Server must be configured as described in the document, "WebSphere Application Server EAL4 – AGD Guidance". In particular, the TOE Single Signon (SSO) must be enabled in the evaluated configuration. In subsequent sections, this document will be referenced as the "User Guidance" document.

The following types of external resources must not be used in the evaluated configuration:

- External Java Authorization Contract for Containers (JACC) provider, including Tivoli Access Manager Server

- External Trust Association Interceptor (TAI) resource

The following types of external resources are optional in the evaluated configuration:

- External Java Authentication and Authorization Service (JAAS) Login module
- External resource adapters
- Embedded WebSphere MQ client

6.2 Product Hypertext Transfer Protocol (HTTP) Server and Product HTTP Server Plug-in

The Product HTTP Server is an HTTP server that is included with the product. This server often is referred to as the "IBM HTTP Server." The Product HTTP Server accepts HTTP requests from web clients and provides support for secure HTTPS connection. The Product HTTP Server can be configured with a Product HTTP Server Plug-in. The Product HTTP Server Plug-Ins component is a set of plug-ins for external HTTP servers. An HTTP Server Plug-in re-routes requests from an external HTTP server to the embedded HTTP server included in the web server container of the Product Application Server component.

The Product HTTP Server and Product HTTP Server Plug-ins supplement the HTTP server built into the Product Application Server web server container. While the embedded web server can serve content, using an external Web Server and Web Server plug-in as a front end to the Web container can provide additional security in a production environment by enforcing secure SSL communications from clients and routing HTTP requests to the Product Application Server..

The Product HTTP Server and Product HTTP Server Plug-in reside in the same process, which is separate from the process in which the Product Application Server resides. The Product HTTP Server receives HTTP requests by remote HTTP Clients. The Product HTTP Server Plug-in forwards the requests to the Product Application Server. The Product HTTP Server enforces secure communication (HTTPS) with cryptographic support from the operational environment: IBM Cryptography for C.

6.3 Product wsadmin Tool

The Product *wsadmin* Tool (henceforth, *wsadmin*) is included in the TOE. Multiple instances of *wsadmin* can be configured in the network or in a single node. Each instance of *wsadmin* runs in its own operating system process and JVM. W*sadmin* is a Java client application. The administrator starts *wsadmin* by running a script (wsadmin.bat or wsadmin.sh, depending on operating system). After *wsadmin* starts, an administrator can use this tool to execute administrative scripting commands for the purpose of managing the Product Application Server. *Wsadmin* must be configured as described in the User Guidance document.

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 the WebSphere Application Server.

Evaluation team testing was conducted at the vendor's development site March 5 through March 9, 2012.

7.1 Developer Testing

IBM's approach to security testing for WebSphere Application Server is security function based. The majority of the testing of the WebSphere Application Server security functions is performed by a series of automated tests. These tests can be mapped to the security functions outlined in the WebSphere Application Server EAL4 Functional Specification document. Together they demonstrate the security relevant behavior of WebSphere Application Server at the interfaces defined in that document: Remote EJB Wrapper Interfaces, Remote HTTP/S Interface, Remote Secure Messaging Interface, Remote IHS-HTTPS Interface, Remote Naming Context Interfaces, Remote ORB Listener Interface, Remote RMIConnectorService Interface, Remote Transactions and Activities Interfaces, Remote UDDI Interfaces, Remote WS-Router Interfaces, and Scripting Interfaces. The goal of the tests is to demonstrate that WebSphere Application Server meets the security functional requirements specified in the ST. The automation framework takes care of test setup, execution and cleanup for all provided tests. The HTTP Header Manual Test Suite is executed by the automation, but requires some user interaction. There are no dependencies between tests unless otherwise noted in a particular test.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite, per the evaluated configuration as described in the IBM WebSphere Application Server Security Target. The tests were run on a selection of the test configurations described in the developer's test documentation. The documentation describes the different test configurations and Editions of the TOE that were used in the test configurations.

The vendor has run all vendor tests on all platforms. The evaluation team executed the majority of the vendor test suite. The team ran a large sample of the vendor test suite since the majority is automated on the Windows and Solaris platforms.

The test environment included the following operating components that are external to the TOE but are required in the TOE's operational environment:

- Microsoft Windows 2008 Server.

The following is a list of additional software that must be installed in the test environment on the STAF server machine.

- STAF (Software Testing Automation Framework) version 3.4.5
- STAF Services

- STAX 3.4.5
- EMS (Environment Management System) 3.4.1
- Event Service 3.1.4
- EventManager Service 3.3.8
- Email Service 3.3.5
- HTTP Service 3.0.2
- CRON Service 3.3.8
- MTS (Manual Test System) Service 3.2.0
- AIS (Automation Infrastructure and Solutions) version 2.2.2
- JDOM 1.0 or higher
- Mantis
- Junit
- Cygwin 1.7.7 (Windows only)
- JDK 1.6
- DB2 v8.12
- Tivoli Directory Server v6.2
- Penetration testing tools such as a scanner and sniffer

The evaluation team performed the following additional functional tests:

- **Access Control (AC.1)–** Confirmed that a user is in the Everyone and/or AllAuthenticatedUsers group(s) and that attempts to access a method which is configured with a permission that denies access to that user ID then the user was denied access to the method.
- **Security Management (SM.1.2) –** Ensured the TOE applies the default settings as advertised in the ST by manually inspected the default mapping of user/group IDs to roles.
- **Cryptographic Support –** Confirmed that that IBM HTTP Server does not accept non-SSL connections on SSL port.
- **New Role Definition –** Confirmed the changes to the restrictions of functionality to roles and functionality allotted to the new Auditor role
- **New Identification logic (Ident.4 and audit) –** Confirmed that for the Ident 4 function in Section 6.1.1.4, "The user ID from the trust token must be in the trusted list of the target server." "The case (2) for testing whether a user ID from the trust token is in the trusted list **does not** generate an audit event.
- **Sort/Search Audit Records**—Determined that some sort and search functionality is available.

- **Validate Application Deployment Permission (Access Control) –** Confirmed that administrators can change application xml file information and these changes are enforced by the TOE. This test also shows that the TOE correctly deploys modified files and correctly parses these xml files.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE, identifying a number of vulnerabilities reported against previous WebSphere Application Server versions. The team verified during examination of the CM system that patches applied to previous versions are automatically included in subsequent versions and therefore are also applied to the TOE.

The evaluation team conducted an updated open source search for vulnerabilities in the TOE, identifying a number of vulnerabilities reported against WebSphere Application Server or operating environment components. The evaluation team determined, through analysis of vulnerability descriptions; consideration of the method of use of the TOE; and with the assistance of IBM developers that only one of these reported vulnerabilities was relevant to the TOE in its evaluated configuration. IBM indicated that an interim fix (iFix) is available to correct the vulnerability. As such the iFix is made part of the TOE and administrators are instructed to download the iFix from IBM.com. The iFix was installed and test demonstrations showed that after the iFix was applied the vulnerability was mitigated.

The evaluation team also performed a port scan of the TOE using Nmap. The evaluation team confirmed that the only open ports identified by the scan were identified in the TOE guidance as allowable open ports or were ports native to the operating system.

In addition to the open source search and port scan, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities. The evaluation team performed tests and/or analysis to confirm:

- The TOE is not susceptible to well known web server vulnerabilities. The team used Wikto to scan the TOE for potential vulnerabilities; three were identified. The team worked with IBM developers to test whether the potential vulnerabilities identified affected the TOE. All were determined not be security relevant and did not affect the TOE. Error code 404 was returned confirming that perl and html are not supported on the TOE.
- The domain separation security of the SDK is enforced as indicated. Applications cannot call protected TOE code because the SDK protects these files. Java security is supported. The property file was examined; it contained TOE files and system code only.
- The meLinkRequest.interface is disabled.

- The connection between a browser and the IBM HTTP Server/HTTP(S) is protected by FIPS certified algorithms and data is not transmitted in the clear.
- The flaws fixed from versions 19 to 21 are not security relevant to the TOE evaluated configuration.

8 DOCUMENTATION

8.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is:

Guidance Documentation	Version	Date
WebSphere® Application Server EAL4 AGD – Guidance (WAS/EAL4/AGD/3.0)	3.0	2012-05-17

This document can be downloaded from http://www.ibm.com/support/docview.wss?uid=swg24030364. This documentation includes

- The Installation and Configuration Guide for the Certified System,
- Administrator's Guide for the Certified System,
- Developers Guide for the Certified System.

The Guidance documentation includes links to pertinent on-line documents in the WebSphere Application Server (WAS) Information Center for "Network Deployment (Distributed operating systems), Version 7.0" at http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/welcome_base.html. The specific online documents cited are:

Online Guidance Documentation	Version	Date
DB2 Information Center http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp		
Express (Distributed operating systems), Version 7.0 http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.javadoc.doc/web/apidocs/overview-summary.html		
IBM HTTP Server for WebSphere Application Server, Version 7.0 http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.ihs.doc/info/ihs/ihs/welcome_ihs.html		
IBM® Tivoli® Directory Server http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm		
Network Deployment (All operating systems), Version 7.0 http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/welcome_ndmp.html		
Network Deployment (Distributed operating systems), Version 7.0 http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html		

Network Deployment (z/OS), Version 7.0
http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.zseries.doc/info/zseries/ae/welcome_zseries.html

System Requirements for WebSphere Application Server V7.0
http://www-304.ibm.com/support/docview.wss?rs=180&uid=swg27012284

WebSphere Application Server (Distributed operating systems), Version 7.0
http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/welcome_base.html

Note that, as User Guidance document covers three evaluated IBM WebSphere Application Server products, some of these references may not be applicable to this particular TOE.

The web pages at the Information Center link also include product information and operating environment information not necessarily specific to the TOE, which have not been evaluated, and should be considered for informational purposes only as they may contain instructions not suitable for use in the evaluated configuration. Only the Guidance documents identified above and the links to web pages within the Installation and Configuration, Administrator, and Developer's Guides should be considered as specific guidance for the TOE.

The following online guidance must not be used: Installing Your Application Serving Environment; and Migrating, Coexisting, and interoperating. In addition the online guidance contains links to pdf files that can be downloaded. These pdf files are not maintained and may contain outdated information. Therefore only the User guidance and the specific web pages identified within the aforementioned guidance document should be used.

8.2 Evaluation Evidence

In addition to the guidance documentation listed above, the following documentation was submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents may be proprietary and not available to the general public. This list does not include small graphics files and email evidence.

Design Documentation	Version	Date
WAS EAL4 LLD Overview of Relevant Components 2 v2.0	2.0	2012-02-15
WebSphere Application Server EAL4 High Level Design WAS/EAL4/HLD/2.0	2.0	2012-02-15
WebSphere Application Server EAL4 Functional Specification WAS/EAL4/FS/2.0	2.0	2012-01-31
WebSphere Application Server Security Architecture ADV_ARC WAS/EAL4/ARC/1.1	1.1	2011-06-13
WebSphere Application Server EAL4 Representation Correspondence WAS/EAL4/RCR/1.1	1.1	2011-06-28
WebSphere Application Server EAL4 Low Level Design Non Relevant	1.1	2011-06-28

WAS/EAL4/LLDNR/1.1

HLD: Jetstream Component High Level Design Topology Routing and Management (TRM)	1.01	2004-10
LLD: ORBExtensions	1.0	2005-07-01
LLD: Overview of the Relevant TOE Components	1.1	2011-06-28
LLD: Activity Service	3.0	2011-08-22
LLD: AdminService	3.0	2008-12-04
LLD: Websphere Common Criteria: Security Auditing	2.0	2011-06-08
LLD: Authentication Service	5.0	2011-08-23
LLD: Common Security Interoperability version 2 (CSIv2)	3.0	2008-10-21
LLD: EJBCollaborator	5.0	2008-12-04
LLD: Enterprise JavaBeans Container (EJB Container)	2.0	2008-11-24
LLD: File Transfer Servlet	2.0	2005-10-27
LLD: HA-Manager	2.0	2005-10-13
LLD: HTTP channel	2.0	2005-03-14
WebSphere Application Server – EAL4 HTTP Server Low Level Design	3.0	2008-12-11
WebSphere Application Server – Messaging EAL4 Low Level Design	5.0	2008-12-15
LLD: NamingProvider	3.0	2008-10-20
WebSphere Application Server Role Based Authorization EAL4 Low Level Design	4.0	2008-12-08
LLD: SSLChannel	3.0	2006-06-21
WebSphere Application Server – EAL4 TCPChannel V6.1 Low Level Design	4.0	2011-07-05
LLD: Transaction Service	3.0	2008-12-23
LLD: UDDI Registry Component	3.0	2011-06-30
LLD: WebCollaborator	5.0	2009-02-17
LLD: WebContainer	4.0	2011-06-30
LLD: Web Services Engine	3.0	2011-06-20
LLD: WSAdmin	4.0	2011-06-10
LLD: WSSecurity	6.0	2011-10-19
LLD: z/OS Proxy Mbean Support	1.0	2006-08-16
WebSphere Application Server EAL4 Low Level Design For The z/Runtime Component	4.0	2008-10-16
WebSphere Application Server for z/OS Version 7.0 Transaction Service LLD – EAL4	5.0	2011-06-28

Selected Source Description WAS/EAL4/SC/1.0	1.0	2011-09-02

Life Cycle Documentation	Version	Date
WebSphere Application Server V7.0.0.19 (32-bit) with APAR PM53930, WebSphere Application Server- Network Deployment V7.0.0.19 (32-bit) with APAR PM53930, and WebSphere Application Server for z/OS V7, service level 7.0.0.19 with APAR PM55522 Configuration List WAS/EAL4/CL/2.7	2.7	2012-05-17
WebSphere Application Server V7.0.0.19, WebSphere Application Server- Network Deployment V7.0.0.19, and WebSphere Application Server for z/OS v 7.0, service level 7.0.0.19 EAL4 Configuration Management WAS/EAL4/ACM/2.0	2.0	2011-05-02
WebSphere Application Server V7.0.0.19, WebSphere Application Server- Network Deployment V7.0.0.19, and WebSphere Application Server for z/OS v 7.0.0.19 EAL4 Life Cycle Management WAS/EAL4/ALC/2.1	2.1	2012-04-18
WebSphere Application Server EAL4 Delivery Documentation WAS/EAL4/ADO/2.0	1.2	2012-03-07
WebSphere Application Server V7.0.0.19, WebSphere Application Server - Network Deployment V7.0.0.19, and WebSphere Application Server for z/OS V7.0.0.19 EAL4 Flaw Remediation WAS/EAL4/FLR/1.2	1.2	2011-11-04
Access List	--	2011-03-22
CMVC 5.0 InfoCenter	--	2003-12-19
Information Technology Security Standards ITCS104	8.0	2010-07-15
Security and Use Standards for IBM Employees ITCS300	12.0	2010-10-15
MD5 Checksum Sample	--	--
Mr. Build Process	--	2005-07-07
Mr. Build Verify	--	2005-11-13
Tequila Functional Specification	3.17	2010-10-15
Download Director Applet Functional Specification	8.30	2010-10-18

Test Documentation	Version	Date
Evaluation Team Test Report For IBM WebSphere Application Server ETR Part 2 Supplement (SAIC and IBM Proprietary)	1.0	2012-03-13
WebSphere Application Server EAL/4 Security Target Functional Tests (ATE_FUN) and Test Coverage Analysis (ATE_COV) WAS/EAL4/ATE/2.1	2.1	2012-03-09

Messaging Security Test Plan for Common Criteria WAS 7.0 EAL4 WAS/EAL4/ATE/3.1/MSGTST	3.01	2011-10-31
Transactions and Activities Test Plan for Common Criteria WAS 7.0.0.19 EAL4 WAS/EAL4/ATE/50/TATP	5.0	2011-10-20
Messaging Admin Scripting Test Suite-EAL4 Test Plan	3.0	2009-01-23
Test output files for supported platforms		

Security Target	**Version**	**Date**
WebSphere Application Server v7.0.0.19 (32-bit) with APAR PM53930 EAL4+ Security Target	3.0	2012-05-17

9 RESULTS OF THE EVALUATION[6]

The evaluation team determined the product to be CC Part 2 conformant, CC Part 3 conformant, and to meet the requirements of EAL 4 augmented by ALC_FLR.2. In short, the product satisfies the security technical requirements specified in "WebSphere Application Server v7.0.0.19 (32-bit) with APAR PM53930 EAL4+ Security Target" on platforms specified in Section 3.3, "Physical Scope."

The evaluation was conducted based upon version 3.1 Revision 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 CCEVS validation team reviewed the evidence provided by the evaluation team, and agreed with their conclusion, and recommended to CCEVS management that an "EAL4 augmented with ALC_FLR.2" certificate rating be issued for WebSphere Application Server v7.0.0.19 (32-bit) with APAR PM53930.

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.

Table 6. TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name

[6] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security Architecture Description
ADV_FSP.4	Complete Functional Specification
ADV_IMP.1	Implementation Representation of the TOE
ADV_TDS.3	Basic Modular Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Production Support, Acceptance Procedures and Automation
ALC_CMS.4	Problem Tracking CM Coverage
ALC_DEL.1	Delivery Procedures
ALC_DVS.1	Identification of Security Measures
ALC_FLR.2	Flaw Reporting Procedures
ALC_LCD.1	Developer Defined Life-cycle Model
ALC_TAT.1	Well-defined Development Tools
ATE_COV.2	Analysis of Coverage
ATE_DPT.1	Testing: Basic Design
ATE_FUN.1	Functional Testing
ATE_IND.2	Independent Testing – Sample
AVA_VAN.3	Focused Vulnerability Analysis

10 VALIDATOR COMMENTS/RECOMMENDATIONS

1. The TOE does not audit all management activities—in particular, it does not audit changes in user access attributes. This may be a concern in environment that have specific auditing requirements.
2. The administrator must ensure that the JVMs used in the environment are trustworthy and regularly patched.
3. Customers are warned that the pdf files available on the IBM website are not necessarily incorrect but are not maintained as an integral part of the set of guidance documentation nor are they part of the evaluated configuration.

11 ANNEXES

Not applicable.

12 SECURITY TARGET

The Security Target for the product evaluation is **WebSphere Application Server v7.0.0.19 (32-bit) with APAR PM53930 EAL4+ Security Target,**Version 3.0, dated May 17 2012.

13 BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, July 2009.
4. Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 3, July 2009.
5. WebSphere Application Server v7.0.0.19 (32-bit) with APAR PM53930 EAL4+ Security Target, Version 3.0, dated May 17 2012