National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

BEA WebLogic Server 8.1 SP5

Report Number: **CCEVS-VR-06-0023**
Dated: **28 April 2006**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Franklin Haskell
The MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

SAIC
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the WebLogic Server TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.2 and International Interpretations effective on 3 September, 2004. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 2 augmented with ALC_FLR.1 family of assurance requirements. The product, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the BEA WebLogic Server 8.1 Security Target. A validator on behalf of the CCEVS Validation Body monitored the evaluation carried out by SAIC. The evaluation was completed in April 2006. Results of the evaluation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report for BEA WebLogic Server 8.1, prepared by CCEVS.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, witnessed testing, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	BEA WebLogic Server V8.1 SP5 with BEA06-81.01 and BEA05-107.00 security advisory patches
Sponsor:	BEA Systems, Inc 2315 North First Street San Jose, CA 95131
Developer:	BEA Systems, Inc 2315 North First Street San Jose, CA 95131
CCTL:	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Kickoff Date:	September 3 2004

Completion Date: 28 April 2006

CC: Common Criteria for Information Technology Security Evaluation, Version 2.2

Interpretations: None.

CEM: Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.2, August 1999.

Evaluation Class: EAL 2

Description: BEA WebLogic Server V8.1 SP5 with BEA06-81.01 and BEA05-107.00 security advisory patches, is an application server that provides a foundation for building and integrating distributed multi-tier applications. It centralizes application services, such as Web server functionality, business components, and access to back-end enterprise systems. It implements Java 2 Platform, Enterprise Edition (J2EE) version 1.3 technologies and provides a complete set of services for J2EE components.

Disclaimer: The information contained in this Validation Report is not an endorsement of the BEA WebLogic Server V8.1 SP5 product by any agency of the U.S. Government and no warranty of the WebLogic Server product is either expressed or implied.

PP: None

Evaluation Personnel: Science Applications International Corporation:
Anthony J. Apted
Keith W. Beatty
Terrie L. Diaz

Validation Team: Franklin Haskell
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

1.2 Interpretations

Interpretation ID	Impact on CC	Impact on CEM Work	Comment

	Requirements	Units	
RI-137	FIA_USB.1 changed	None	Applied

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 2 – Threats

Threat Identifier	Threat Description
T.BYPASS	An attacker may be able to bypass TOE protection mechanisms through unprotected interfaces in order to inappropriately access protected data and services.
T.EXCESS_AUTHORITY	An unauthorized user may be able to exercise administrator authorities to inappropriately manage the TOE.
T.NO_TIME	Those responsible for the TOE may not be able to determine the sequence of audited security relevant events.
T.NOCRYPTO	An attacker may be able to observe authentication data transmitted in the clear due to cryptographic services not being available.
T.STORAGE	An attacker may be able to cause the loss or destruction of Audit and other TSF data.
T.TAMPER	An attacker may be able to inappropriately modify or otherwise tamper with TSF programs and data.
T.TSF_COMPROMISE	A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNACCOUNTABLE	Users of the TOE may not be held accountable for their security-relevant actions.
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policies.
T.UNDETECTED_ACTIONS	The administrator may not have the ability to detect potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNIDENTIFIED_USERS	An attacker may gain access to the TOE without being reliably identified allowing them to gain unauthorized access to data or TOE resources.

2 Identification

The product being evaluated is **BEA WebLogic Server V8.1 SP5**.

3 Security Policy

There are no specific security policies that the evaluated product enforces. It does enforce user security policies as described in the Security Target.

3.1 Access Control

Policies are created by the user but use attributes maintained by the product: username, group membership, role, resource type, resource identity, and time of day. The resources to which access is permitted or denied include Java constructs (beans, APIs, jars, etc.), the administrative console, and servers. Note that certain resources allow access based upon the operation being requested. This capability is not mentioned in the ST nor was any comprehensive testing of it performed; therefore no statements can be made regarding it in this Validation Report.

3.2 Identification and Authentication

The TOE supports multiple identification and authentication mechanisms: username and password; token-based (using either X.509 certificates or CORBA Common Secure Interoperability version 2 (CSIv2) identity assertion); and credential mapping which provides a capability by which legacy applications use their own I&A mechanisms to authenticate to a WLS resource.

3.3 Auditing

The TOE generates audit records of security relevant events as they occur within the security framework. They are stored by the underlying operating system and, hence, the TOE is dependent upon that OS for proper protection of the audit trail.

4 Assumptions

4.1 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Physical Assumptions

Assumption Identifier	Assumption Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the IT environment.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 4 – Personnel Assumptions

Assumption Identifier	Assumption Description
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

4.3 Operational Assumptions

The following operational assumptions are identified in the Security Target:

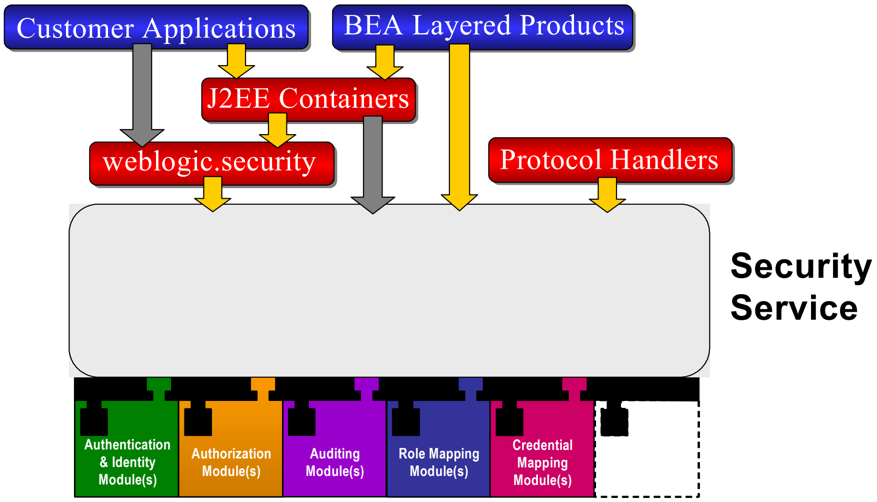
Table 1 – Connectivity Assumptions

Assumption Identifier	Assumption Description
A.NO_UNTRUSTED	There are no untrusted user accounts or malicious software on the server platform.

5 Architectural Information

WebLogic Server (WLS) consists of a single distinct subsystem. The figure below shows a 'Security Service' which includes the basic 'Security Framework' of the WebLogic Server and a series of security service provider 'modules' (note that the security provider modules in the figure are only examples). The Security Service and the following associated modules: audit, authorization, role mapping, adjudication, authentication, identity assertion, and credential mapping form the TOE; while the other entities in the figure depicted above the Security Service are examples of applications supported by the TOE.

Generally, user requests will come in from the network and will be handled by the security framework provided by WebLogic Server. Customer applications are acquired and installed by WLS administrators so that the appropriate controls are configured and subsequently enforced before the applications can be accessed.



6 Documentation

The following documents are available to customers and are pertinent to the installation, configuration, and operation of the TOE. All of these can be found at http://e-docs.bea.com.

- Installing BEA WebLogic Platform 8.1 SP 5, 5 Oct 2005
- Administration Console Online Help (http://e-docs.bea.com/wls/docs81/ConsoleHelp/index.html)
- Configuring and Managing WebLogic Server 8.1, 23 Sep 2005
- Developing Web Applications for WebLogic Server 8.1, 26 Sep 2005
- Introduction to WebLogic Security 8.1, Aug 2005
- Managing WebLogic Security 8.1, 9 Dec 2004
- Programming WebLogic Enterprise JavaBeans 8.1, 13 Dec 2005
- Programming WebLogic jCOM 8.1, 28 Feb 2003
- Programming WebLogic Security 8.1, Aug 2005
- Programming WebLogic Server J2EE Connectors 8.1, 1 Jul 2003
- Programming WebLogic Web Services 8.1, 25 Jun 2004
- Securing a Production Environment 8.1, 21 Jun 2004
- Securing WebLogic Resources 8.1, 14 May 2004
- WebLogic Server Command Reference 8.1, 15 Mar 2004

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. All testing took place on Dell Latitude Laptops running the following combinations of software:

- Windows 2003 with JRockit 1.4.2_08
- Windows XP with JRockit 1.4.2_08
- Sun OS 5.8 sparc with Sun Java 2 SDK 1.4.2_08.

7.1 Developer Testing

The vendor ran the automated test suite in various configurations, consistent with the test environment described in the Testing Documentation, and gave the evaluation team the actual results. The test configurations were representative of both the operating systems supported and the application environment (JVM). 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 evaluation team devised a test subset based on coverage of the security functions described in the ST. The vendor test system was used with team generated test procedures and team analysis to determine the expected results. All actual results matched the expected results.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product and found none not already known to and addressed by the developer through security advisories and patches. They also examined the vendor's vulnerability assessment and identified three vulnerabilities relevant to the evaluated version of the TOE in its evaluated configuration. The team testing showed that either the vulnerability was not present in the evaluated configuration or that a patch was available.

8 Evaluated Configuration

The evaluated configuration is the Java 2 environment. The BEA JRockit 1.4.2_08 SDK and Sun Java 2 SDK 1.4.2_08 with Java HotSpot™ Client VM are specifically supported. As customer applications and dataset sizes vary tremendously no configuration guidelines can be given here. Potential customers are encouraged to seek very competent assistance to size their hardware.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2 and CEM version 2.2. The evaluation determined the BEA TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements augmented with ALC_FLR.1. The rationale supporting each CEM work unit verdict is recorded in the **Evaluation Technical Report for the WebLogic Server 8.1 SP5 Part 2** which is considered proprietary.

10 Validator Comments/Recommendations

BEA WebLogic Server is a product with functionality intended to provide frameworks for managing access to: data, data structures, and application components supporting both new applications and existing ones connecting over networks. As such its implementation has to be robust.

The validation team believes that the claims made and successfully evaluated for the product represent a set of requirements that are a reasonable selection covering, to a certain depth, the functionality of the product. The product, while extensive in functionality, only runs at the application level. It relies upon the underlying operating system for several types of support: audit review and storage, cryptographic facilities, security management, time stamps, and separation of the product and its users. Also, the usual training and physical assumptions apply. Because of this product construction, purchasers should be very careful to follow the configuration guidance. Controlling access, both physical and network, is very important; as is the injunction not to allow anything other than WLS to run on the server machine.

No claims are made for the network connections that must be in place between remote applications and the server or those between servers on different machines. It is up to the customer to put measures in place to appropriately secure these data paths.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **BEA WebLogic Server 8.1 Security Target**, Version 1.0, dated May 22, 2006.

13 Glossary

No definitions beyond those in the CC or CEM are supplied.

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.2, January 2004, CCIMB-2004-01-001.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.2, January 2004, CCIMB-2004-01-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.2, January 2004, CCIMB-2004-01-003.

[4] Common Methodology for Information Technology Security: Evaluation Methodology, Version 2.2, January 2004, CCIMB-2004-01-004.

[5] Evaluation Technical Report for BEA WebLogic Server 8.1 SP5 Part 1, Version 0.2, 24 April 2006.

[6] Evaluation Technical Report for BEA WebLogic Server 8.1 ETR Part 2, Version 0.2, 24 April 2006.

[7] Evaluation Team Test Report for BEA WebLogic Server 8.1 SP5 Part 2 Supplement, Version 0.1, 24 February 2006.

[8] BEA WebLogic Server 8.1 Security Target, Version 1.0, 22 May 2006.

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