National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

BladeLogic Operations Manager 7.4.2

Report Number: CCEVS-VR-VID10206-2009
Version 1.0
11 November 2009

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

1 Executive Summary

The Target of Evaluation (TOE) is version 7.4.2 of the BladeLogic Operations Manager product. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in November 2009. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.3 and the Common Methodology for IT Security Evaluation (CEM), Version 2.3. The evaluation was for Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1 (Basic Flaw Remediation). 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).

BladeLogic Operations Manager product provides a data center configuration management solution for remote servers. It allows enterprise administrators to view and manage server configurations, deploy software and complex packages of files and server assets, store server configurations, and compare servers to detect discrepancies in their configurations. The BladeLogic Operations Manager product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The *BladeLogic Operations Manager Version 7.4.2 Security Target version 2.0, dated 11 November 2009* identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the BladeLogic Operations Manager product by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Evaluated Product	BladeLogic Operations Manager 7.4.2
Sponsor & Developer	BMC Software, Houston TX
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	November 2009
CC	*Common Criteria for Information Technology Security Evaluation*, Version 2.3, August 2005
Interpretations	None.

CEM	*Common Methodology for Information Technology Security Evaluation*, Version 2.3, August 2005
Evaluation Class	EAL3 Augmented with ALC_FLR.1
Description	The TOE is the BladeLogic Operations Manager 7.4.2 software, which is a Network Management system developed by BMC
Disclaimer	The information contained in this Validation Report is not an endorsement of the Operations Manager product by any agency of the U.S. Government, and no warranty of the Operations Manager product is either expressed or implied.
PP	None
Evaluation Personnel	Chris Gugel Matthew Leiseth John Schroeder Amit Sharma
Validation Body	NIAP CCEVS

2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

Users, whether they be malicious or non-malicious, could attempt to modify the configuration of remote servers on a local network in an attempt to reduce the security posture of those remote servers.
An administrator may incorrectly configure the TOE to mismanage user accounts or adhere to noncompliant security and/or regulatory policies.
An authorized user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
Users, whether they be malicious or non-malicious, could attempt to misconfigure or modify their user accounts in an attempt to tamper with TOE resources or modify security information relative to the TOE.
A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
Users, whether they be malicious or non-malicious, could gain unauthorised access to the TOE by bypassing identification and authentication countermeasures.
Malicious users could monitor (e.g., Sniff) network traffic in an unauthorized manner.
Users could gain unauthorised access to the web resources by bypassing identification and authentication requirements.

3 Identification

The product evaluated is BladeLogic Operations Manager 7.4.2.

4 Security Policy

4.1 Access Control

The TOE enforces a BladeLogic Role Based Access Control (RBAC) Policy, which works with Object based Permissions to restrict access to the management functions of the TOE based on roles and objects. (see section 6.1.2.2 for more information on Object based Permissions)

Once a client-tier user has authenticated to a middle-tier server, an active role must be established for the authenticated identity. The BladeLogic Core Database also records the set of roles in which each registered BladeLogic user is authorized to operate. Subsequent to successful user authentication, client and middle-tier entities negotiate an active role for the current session. Role negotiation is secured via user data protection (encryption of protocol exchanges), employing TLS.

Once access is granted and an authorized role has been negotiated, a user is limited to only management functions that are controlled by the authorizations assigned within the active role.

The TOE's RBAC system provides the ability to define levels of authority for users. A user operating within the RBACAdmins role has the ability to define roles and authorizations and have complete control over the TOE. It is through the use of roles, objects and assigning authorizations to various roles that users are granted access within BladeLogic Operations Manager Version 7.4.2. All discussion of "security privileges" within this document should be understood to mean Roles and their associated authorizations to access various parts of the TOE. Access to resources on managed servers is also under the control of the TOE's RBAC system. The TOE manages access control lists (ACLs) on each of the managed servers in the server tier. RSCD agents (which fall within the TOE) residing on each of these managed servers refer to their centrally managed ACL to determine whether an incoming management command is authorized and what local user to map to (i.e., impersonate) when servicing that management request. Each incoming command identifies the BladeLogic user identity and RBAC role for which the Application Server is issuing the management command. The ACL maps the pairing of incoming user identity and RBAC role to a local user recognized by the managed server's host operating system. The RSCD management agent then impersonates the mapped local user when servicing the particular request. In this way, the TOE leverages the user-based access control mechanisms provided by the managed server's operating system, which is part of the IT environment.

4.2 Identification and Authentication

The TOE requires users to provide unique identification and authentication data prior to being granted any administrative access to the system. The TOE enforces a BladeLogic Role Based Access Control Policy, which restricts access to the management functions of the TOE. This protection requires that users of the TOE be authenticated prior to any access to the management functions is granted.

The TOE provides the functionality of counting unsuccessful authentication steps, and when a user meets a specified number they are locked out for a specified amount of time. Additionally, the TOE verifies a user's password meets complexity requirements before it is changed.

The TOE provides two authentication mechanisms, Secure Remote Password and Active Directory / Kerberos. The Configuration Manager contains client- side implementations of these two authentication mechanisms, however, only Secure Remote Password is utilized in the TOE's evaluated configuration. After successfully authenticating a Configuration Manager user, the Application Server issues the client a BladeLogic Single Sign-on (SSO) credential. This SSO credential can be stored in process memory or on the local file system. Once the SSO credential is stored, it can be picked up and used by the Configuration Manager as well as BLCLI for future session establishment. The middle-tier's BladeLogic Application Server and BladeLogic Reports Server contain server-side implementations of these two authentication mechanisms.

SRP users are registered within a BladeLogic users table maintained within the BladeLogic Core Database. These user records include the authenticators used to authenticate users via the SRP authentication protocol.

4.3 Security Management

The TOE is managed through the Configuration Manager or BladeLogic CLI. Two default user roles exist out of the box: BLAdmins to perform job management and RBACAdmins to manage users, roles, auditing, and other internal configuration issues. Additional roles can be added and issued sets of authorizations.

Many operations which can be performed using the Configuration Manager can also be performed via the BladeLogic CLI, but the Configuration Manager offers additional functionality not available on this interface. As a result, the Configuration Manager is the typical mechanism used to manage the TOE.

4.4 Audit

The TOE maintains multiple types of audit logs for forensics purposes. Job logs and Authorization logs record actions performed on the Configuration Manager or BladeLogic CLI. The actions recorded are based on the authorizations defined by the TOE. Accessed authorizations, whether accepted or rejected, are logged.

Agent logs are written to remote servers and record information about operations of those remote servers. This data is also written to the Reports Server and is used in generating reports.

4.5 Protected Communications

The TOE uses the BladeLogic Reports Server to support protection of external TOE communication via a web browser used by Reports Server by performing TLS v1.0 encryption through the Apache OpenSSL-based cryptographic module (mod_SSL). v0.9.7l). The BladeLogic Reports Server resides on a Tomcat Apache server v4.1.31. A username and password request is issued by the web server. The user provides an SRP username and password to the web server which is passed to the Apache server via an industry standard web browser, either Internet Explorer v6 or Netscape v7. The Reports Server conducts an SRP authentication exchange with the Application Server, using the username and password provided over the web interface. The Application Server will validate the users claimed credentials against password and usernames stored in the SQL Server database. The TOE will return the success or failure of the authentication process. The Apache server is configured to use the strongest form of TLS security and relies on the user's web browser in the IT environment to negotiate the TLS protocol with its associated cryptography to perform the TLS handshake for authenticating the end points of the communication channel and to encrypt the data.

The BladeLogic Core Database stores the SRP authenticators in the SQL Server Database which the Application Server require to authenticate client users. The TOE relies on the DBMS, an element of the IT environment, to protect the integrity and confidentiality of these client authenticators, as well as other user record attributes that may affect an SRP user's ability to log into the system (e.g., lockout status, password expiration time, etc.). Note that the SRP authenticator is essentially a cryptographic hash of the SRP password along with other account data. A user's SRP password cannot be retrieved from the authenticator.

5 Assumptions

5.1 Personnel Assumptions

Table 1 – Personnel Assumptions

One or more authorised administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.
System Administrators exercise due diligence to update the TOE with the latest patches and patch the IT Environment (e.g., OS and database) so they are not susceptible to network attacks.

5.2 Physical Assumptions

There are no physical assumptions for the TOE.

5.3 Logical Assumptions

Note that the following assumption governed testing of the TOE. Operations Manager is capable of managing servers in a DMZ if client-site certificate authentication is configured for those servers.

Table 2 – Logical Assumptions

The network servers that the TOE will monitor and manage are isolated from any other network, either by physical separation or using logical protection such as a firewall.

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see section 4).

The evaluated configuration of the TOE includes the BladeLogic Operations Manager 7.4.2 application that is comprised of the following:

- **Configuration Manager –** a GUI-based system for automating management of remote servers.
- **BladeLogic CLI –** A command line interface that allows access to the Configuration Manager to perform most procedures.
- **Network Shell –** A network-aware shell that allows cross-platform access through a command line interface.
- **BladeLogic Application Server –** A server that provides Configuration Manager access to RSCD Agents and can run ad-hoc and scheduled automation tasks against RSCD agents.
- **BladeLogic Reports Server –** A web-based reporting engine that supplies pre-created and ad-hoc reports on server inventory, compliance, activity, etc.
- **Remote System Call Daemon (RSCD) Agent –** The BladeLogic Agent that runs on all managed servers, providing the ability to manage them remotely.
- **BladeLogic Core Database –** Application interface between the Application Server and the SQL Database. The Core Database is used to store configuration and event data used by other BladeLogic Operations Manager components.
- **BladeLogic Reporting Data Warehouse –** Application interface between the BladeLogic Reports Server. The Reporting Data Warehouse is used to retrieve stored data that contains event information and storage of audit reports.

The scope and requirements for the evaluated configuration are summarized as follows:

1. The Operations Manager 7.4.2 software (i.e., the TOE) will be installed with the following division of components:
   - RSCD Agent, Configuration Manager, BladeLogic CLI, Network Shell, BladeLogic Application Server, and BladeLogic Core Database
   - BladeLogic Reports Server and BladeLogic Reporting Data Warehouse

- RSCD Agent

Note that the server running the Configuration Manager is required to have an RSCD agent installed on it as well. RSCD Agents must be installed on all systems which are to be managed remotely.

2. The TOE requires a SQL database to be installed which functions as the BladeLogic Core Database. The test environment utilized SQL Server 2005.

6.1 System Requirements

This section identifies the hardware and software requirements for the platforms described in the evaluated configuration. The TOE was evaluated using Windows Server 2003 for its management capabilities, and Windows Server 2003, Red Hat Advanced Server 4.0, and Solaris 9 for RSCD agents. The minimum system requirements for each component are illustrated below:

BladeLogic Component	Server OS Requirements	Processor/Speed	Memory	Disk Space	Screen
Configuration Manager, Network Shell (NSH), BladeLogic CLI	**Windows 2003 Server**	**• minimum - Intel Pentium III, 500 MHz • recommended - Intel Pentium IV, 2 GHz or better**	**• minimum - 256 MB • recommended - 512 MB or better**	**200 MB**	**• 1024 x 768 • minimum 256 colors**
Reports Server	**Windows 2003 Server**	**minimum - 1 Xeon, 1.5 GHz • recommended - 2 Xeon, 2 GHz or better**	**• minimum - 1 GB • recommended - 2 GB or better**	**10 GB**	**N/A**
Application Server	**Windows 2003 Server**	**• minimum - 2 Xeon, 2 GHz • recommended - 4 Xeon, 3 GHz or better**	**• minimum - 1 GB • recommended - 4 GB**	**50 GB**	**N/A**
RSCD Agent	**Windows 2003 Server, Solaris 9.0 Server, or Redhat AS/ES 4.0 Server**		**1MB**	**10MB**	

7 Architectural Information

The TOE maintains a three-tier architecture that consists of client, server, and middle tiers. Figure 1 illustrates the relationship between the major components of the three-tiered BladeLogic system used for the evaluated configuration of the TOE.

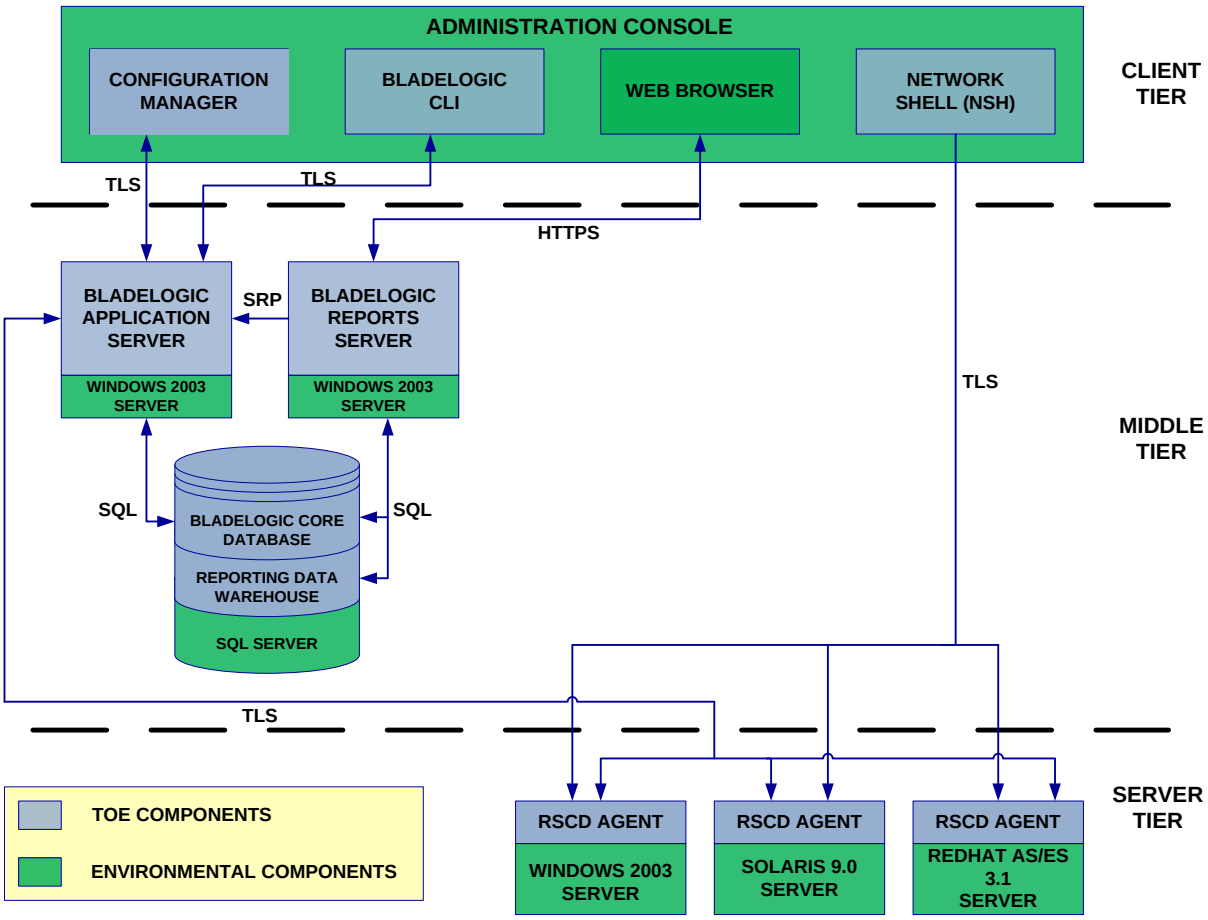

Figure 1 – BladeLogic Operations Manager Version 7.4.2 TOE Boundary

7.1.1 TOE Client Tier

The client tier provides three types of administrative management consoles: Configuration Manager, BladeLogic CLI, and Network Shell. In the evaluated configuration, all of BladeLogic's client-tier applications run on top of a Microsoft Windows 2003 server platform that allows for the management of the Middle and Server Tier components.

7.1.2 TOE Middle Tier

The middle tier provides the communications protocols and management of communications. In addition, the middle tier controls the Configuration Manager's interaction with the database and provides instructions on issuance of operating systems and applications to the RSCD Agent servers.

All clients and servers are set to communicate using secure communication based on Transport Layer Security (TLS). TLS automatically negotiates the strongest form of encryption that clients and servers can support. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic

standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1.3 TOE Server Tier

The TOE's server tier consists of RSCD Agents on remote servers that run Solaris 9.0 Server, RedHat AS/ES 4.0 Server, and Windows 2003 Server.

7.2 TOE Components

7.2.1 BladeLogic Configuration Manager

The Configuration Manager is a GUI that server administrators use for managing and automating data center procedures Once the user has been authenticated, their actions upon objects/resources are controlled via the BladeLogic Role Based Access Control Policy; all authorizations that allow access to these objects/resources is controlled by this policy.

7.2.2 BladeLogic CLI

BladeLogic's CLI allows BladeLogic users to perform most procedures available in Configuration Manager from a command line rather than using the Configuration Manager console. This interface requires the user to authenticate to the BladeLogic Application Server. Once the user has been authenticated, their actions upon objects/resources are controlled via the BladeLogic Role Based Access Control Policy; all authorizations that allow access to objects/resources is controlled by this policy.

7.2.3 BladeLogic Network Shell

Network Shell (NSH) is a network-aware shell that enables cross-platform access through a command line interface. In the evaluated configuration, the NSH directly connects to the RSCD Agent(s) using Self-signed, client-side certs over a TLS connection. The Self-signed, client-side certs enable agents to authenticate NSH clients. To accomplish this, agents are provisioned with SHA1 fingerprints of NSH clients' self-signed certificates. The user may then connect to any server with the BladeLogic agent installed that has been provisioned with the fingerprint of the user client's certificate. Once an NSH client has connected to an agent, the client's authorizations are enforced by configuration files (ACLs) stored on each server.

Note: A default installation of BladeLogic provides no authentication. Instead, this configuration relies on the host operating system of the Network Shell client to authenticate a user. A Network Shell proxy can be used to leverage BladeLogic authentication with this application, but it was not included in the evaluated configuration and should only be employed at the administrator's risk.

7.2.4 BladeLogic Application Server

The Application Server is the fundamental component in the BladeLogic Architecture. The Application Server allows users, through the Configuration Manager console to: browse configurations on servers in real time (i.e., snapshot), audit configurations on servers against other servers or against a baseline (i.e., audit job), run compliance policies

against servers, install software and patches, and run scripts against servers (outside of the scope of the evaluated configuration). In addition to communicating between the Administrative console components and RSCD Agent servers, the Application Server also controls Configuration Manager's interaction with the BladeLogic Core Database. The BladeLogic Application Server utilizes TLS for session-layer security when communicating with the Configuration Manager and BladeLogic CLI in the client tier and RSCD agents in the server tier.

7.2.5 BladeLogic Core Database and the Reporting Data Warehouse

There are two distinct databases, the core database and the data warehouse. The AppServer accesses the core database; the reports server accesses the data warehouse. Data is aggregated and written to the data warehouse from the AppServer via NSH Script jobs that perform the ETL operations.

7.2.6 BladeLogic Reports Server

BladeLogic Reports Server is a web-based reporting utility that allows users to view pre-existing or ad-hoc reports created by running one of the many types of jobs that BladeLogic is capable of executing. Users access it using a local web browser over Hyper Text Transfer Protocol Secure Socket (HTTPS). BladeLogic Reports Server uses the Application Server to authenticate users, and it reads compliance data, job run data, and user log data (i.e., audit trails) from the Reporting Data Warehouse.

7.2.7 BladeLogic RSCD Agent

An RSCD Agent runs as a daemon (UNIX) or a service (Windows) on all servers managed by BladeLogic. The RSCD Agent software allows a client (BladeLogic Application Server or Network Shell computer) to establish contact with the RSCD Agent computer. The RSCD agent runs commands on behalf of the BladeLogic Application Server and sends the results back to the Application Server. It never initiates a connection to the Application Server, but only communicates when first contacted by the Application Server. The configuration of the RSCD Agent software determines whether a client can establish a connection to the RSCD Agent and what permissions the client will have.

8 Documentation

The documents were evaluated to satisfy assurance requirements:

Component	Document(s)	Rationale
ADO_DEL.1: Delivery procedures	**[1] BMC/BladeLogic Electronic Product Distribution (EPD)**	This document describes product delivery for BladeLogic and a description of all procedures used to ensure objectives are not compromised in the delivery process.
ADO_IGS.1: Installation, generation, and start-up procedures	**[1] BladeLogic Administration Guide v7.4.2** **[2] BladeLogic Users Guide v 7.4.2** **[3] BladeLogic Installation Guide v7.4.2** **[4] Using BladeLogic Reports** **[5] BladeLogic Operations Manager Install Guide.doc**	These documents together document the procedures necessary and describe the steps required for the secure installation, generation, and start-up of the TOE.
AGD_ADM.1: Administrator guidance	**[1] BladeLogic Administration Guide v7.4.2** **[2] BladeLogic Users Guide v 7.4.2** **[3] BladeLogic Installation Guide v7.4.2** **[4] BladeLogic Network Shell Command Reference v 7.4.2** **[5] Using BladeLogic Reports** **[6] Booz Allen_BMC_v7+4+2_1-3_AdminGuideSupp_3_20091106.doc**	These documents together describe the processes to be used for proper administration of the TOE.
AGD_USR.1: User guidance	**[1] Using BladeLogic Reports** **[2] BladeLogic Users Guide v 7.4.2**	These documents together describe the proper use of the TOE from a user standpoint.

Table 8 – Assurance Documents Evidence

These documents are provided to customers who have purchased the TOE.

9 TOE Acquisition

The NIAP-certified Operations Manager product is acquired via normal sales channels, and digital delivery of the TOE is coordinated with the end customer by BMC.

10 IT Product Testing

The test team's test approach is to test the security mechanisms of the BladeLogic Operations Manager by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, High Level Design (HLD), Functional Specification (FSP), and the vendor's test plans were used to

demonstrate test coverage of all *appropriate* EAL3 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team created a test plan that contained the vendor functional test suite, and supplemental functional testing of the vendors' tests. Booz Allen also performed vulnerability assessment and penetration testing.

10.1 TEST METHODOLOGY

10.1.1 Vulnerability Testing

The evaluation team executed the following vulnerability tests against BladeLogic Operations Manager Version 7.4.2:

- Eavesdropping on Communications (wireshark v1.0)
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning (nmap v4.60)
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Buffer Overflow / Format String / Unexpected Input Attack (CIRT.dk fuzzer v1.0)
  In this attack, the evaluators attempted to discover and exploit any software errors that do not appropriately handle various non standard inputs. The evaluators attempted to inject known malicious inputs into the various TOE interfaces. These malicious inputs form 3 categories.
  - Buffer Overflows: In this case, larger and larger inputs are injected to try to overflow a buffer and corrupt the program stack.
  - Format Strings: In this case, format strings are injected to attempt to see if they are not handled correctly by the program.
  - Special Characters: In this case, unexpected special characters are injected in an attempt to induce non standard behavior.
- ICMP Blind Connection Reset (icmp-reset v1.0)

This test attempted to exploit a known vulnerability using ICMP connection reset packets. If effective, this test would prevent the normal functionality of the TOE and invoke a denial of service against it.

- Generic Vulnerability Scanner (nessus v3.2.1.1)

  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that include the following:

Backdoors	Gain root remotely	RPC
CGI abuses	General	Settings
Denial of Service	Miscellaneous	SMTP Problems
Finger abuses	Netware	SNMP
Firewalls	NIS	Untested
FTP	Port scanners	Useless services
Gain a shell remotely	Remote file access	

- TCP Malformed Packet Flooding (tcpsic/isic v1.0)

  This test attempted to shutdown TOE resources by flooding the network with large amounts of malformed tcp packets.

- Unauthenticated Access / Directory Traversal Attack (standard browser)

  This test used "URL hacking" to attempt to access protected TOE resources by injecting unexpected input into requests that were sent to the TOE. This was done using two different approaches to URL exploitation.
  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).

- SQL Injection / Cross Site Scripting Attack (Paros v3.2.13)

  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were input into the various fields and variables and the output was analyzed for inconsistencies.

- Web Server Vulnerability Scanner (nikto v2.02)

  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

File Upload.	Denial of Service.
Interesting File / Seen in logs.	Command Execution / Remote Shell.
Misconfiguration / Default File.	SQL Injection.
Information Disclosure.	Authentication Bypass.
Injection (XSS/Script/HTML).	Software Identification
Remote File Retrieval	Remote source inclusion.

- Documented Web Server Vulnerabilities (standard browser)

This test attempted to exploit publicly known vulnerabilities that potentially exist in the web server of the product.

- Database Impersonation (socat v1.4.0.3 / CIRT.dk fuzzer v1.0)
  This test attempted to impersonate the TOE database system and provide unexpected input back to the TOE.
- Client Authentication Attack (raw product binaries)
  This attack tested the TOE's ability to authenticate remote machines connecting to a system via the network shell. This test attempted to authenticate using no certificate or using an attacker generated self signed certificate.
- Protocol Attack – Denial of Service (shell script using netcat v1.0)
  This test attempted to interrupt the communications between various TOE components by connecting to TOE servers using nonstandard clients.

10.1.2 Vulnerability Results

The following lists any issues that were discovered as a result of the vulnerability testing process. These issues along with the related guidance for mitigation have been included in the Common Criteria Addendum to the product Administrator Guidance.

- *Use of Dangerous HTTP Methods*

The default installation of Apache Tomcat used for the Bladelogic Reports server allows several unneeded HTTP methods that are considered to be dangerous in a deployed system. Administrators are advised to disable the following HTTP methods:

HTTP PUT
HTTP TRACE
HTTP DELETE

This issue has been mitigated by the inclusion of the guidance addendum.

- *SSL Cipher Suites*

The default installation of Apache Tomcat used for the Bladelogic Reports server allows the use of low strength SSL cipher suites with HTTPS. Administrators are advised to limit the acceptable cipher suites to the following suite:

TLS_RSA_WITH_AES_256_CBC_SHA

This issue has been mitigated by the inclusion of the guidance addendum.

- *Additional Consoles*

The default installation of Apache Tomcat used for the Bladelogic Reports server contains two additional non-standard web consoles. The first is a Tomcat administrative console and can be found by entering /admin after the web server URL. This console does not have any valid login by default. The second is a third party middleware console and can be found by entering /scopeserver after the web server URL. This console has the same login credentials as the standard Report Server interface. Administrators are advised to restrict all remote access to these consoles at a minimum and are recommended to undeploy and remove them entirely from the Tomcat root directory. All configurations should be done locally in order to ensure a secure configuration.

This issue has been mitigated by the inclusion of the guidance addendum.

- *Tomcat Web Root*

Administrators should be aware that it is possible for a remote web user to obtain the absolute path of the Tomcat web root directory on the web server machine. This information is leaked in an error message that is triggered when a specific invalid resource is accessed. Administrators are advised not to rely on the confidentiality of the Tomcat web root for any security related activity or application.

This issue is considered to be an Acceptable Residual Vulnerability in the system. This issue is a leak of information only. By itself it does not yield any exploitable vulnerability and would have to be used in conjunction with some other exploit.

- *Database Location*

Administrators should be advised to connect the Bladelogic Server and its backend Database Server on the same LAN or on an isolated management LAN. It is imperative that all machines connected on this network are considered to be trusted and non malicious. The server communicates with the database using protocols that do not protect the confidentiality of the data being transmitted, to include database passwords. This data is limited to the LAN on which the server and database are installed. The LAN should therefore be protected accordingly.

This issue is considered to be an Acceptable Residual Vulnerability in the system, but the inclusion of the additional guidance minimizes the impact of this issue.

- *Agent Connectivity*

Administrators should be advised that the environment should restrict the ability to connect to the Agent machines on the Bladelogic communication port to the Bladelogic server only. There exists a case whereby a third party can disrupt the communications between the server and its Agents by connecting directly to the Bladelogic communication port on the Agent machines. An administrator could restrict this access using a local or remote firewall solution with rules allowing only the Bladelogic server access or by utilizing a dedicated management LAN for the purpose of administering Bladelogic Agents.

This issue is considered to be an Acceptable Residual Vulnerability in the system, but the inclusion of the additional guidance minimizes the impact of this issue.

- *Network Shell Authentication*

Administrators should be aware that the authentication of incoming connections over the network shell is not enabled by default. Administrators must configure the product to use TLS with client side certificates in order to ensure the security of the systems on which Bladelogic Agents are installed. Without this configuration, any 3rd party could gain a remote shell on an Agent machine unauthenticated.

This issue has been mitigated by the inclusion of the guidance addendum.

Alternatively, NSH Proxy usage can force SRP authentication onto the NSH via the application server. However, this functionality was not tested as part of the evaluation and should only be used if an administrator is willing to accept this risk.

All issues have either been mitigated by the inclusion of guidance or are considered to be Acceptable Residual Vulnerabilities in the system.

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the BladeLogic Operations Manager 7.4.2 TOE meets the security requirements contained in the Security Target.

The criteria against which the BladeLogic Operations Manager 7.4.2 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the BladeLogic Operations Manager 7.4.2 TOE is EAL 3. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in November 2009. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

12 Validator Comments/Recommendations

The following items below are recommendations for usage of the TOE that have been derived from testing. They have been incorporated into the supplemental administrative guidance.

- It is recommended that the TOE be managed exclusively using the Configuration Manager application. BLCLI does not afford any additional management functionality and lacks some capabilities that the CM has such as the built-in Network Shell. As a result the primary focus of testing was the Configuration Manager.
- It is recommended that direct access to the Network Shell executable be restricted. Administrators of the TOE should be required to use the Configuration Manager application to execute Network Shell commands. By doing this, individual administrators can be restricted to certain system-level privileges or denied access entirely based on their role within the Configuration Manager.
- It is recommended that an administrator not be given the ability to decommission and create servers. This should be the responsibility of the super user (BLAdmins) role. The reason for this is that the BLAdmins role can be locked out of being able to configure servers if another role adds them to the list of available servers.

- It is recommended that OpenSSL be upgraded in all cases, as a precaution.
- The system administrator should implicitly follow the instructions in BladeLogic Operations Manager v7.4.2 Admin Supplemental Guidance, Version 1.3, November 6, 2009 to mitigate the impact of know vulnerabilities listed in Section 10.1.2, Vulnerability Results.

13 Annexes

Not applicable.

14 Security Target

The security target for this product's evaluation is BladeLogic Operations Manager Version 7.4.2 Security Target *version 2.0, dated 11 November 2009.*

15 List of Acronyms

Acronym	Description
ACL	Access Control List
AES	Advanced Encryption Standard
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CLI	Command Line Interface
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTPS	Hyper Text Transfer Protocol Secure Socket
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
PXE	Preboot Execution Environment
RBAC	Role-Based Access Control
RSCD	Remote System Call Daemon
SRP	Secure Remote Password
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

16 Terminology

Server:	A server is a machine where Remote System Call Daemon (RSCD) Agent software was installed.
Client:	Machines that are running Configuration Manager, or Network Shell.
Provisioning:	The remote installation of operating systems or applications from the Application server to an RSCD Agent Server.
RBACAdmins:	A built-in role with authorizations granting the user in this role permission to read and modify ACL authorizations for all system objects in BladeLogic.
RBACAdmin:	The built-in user which is assigned the RBACAdmins role.
BLAdmins:	A built-in role with authorizations granting the user in this role permission to change permissions for all system objects.
BLAdmin:	The built-in user which is assigned the BLAdmins role.
Roles:	A role is an organization entity such as administrators or database managers.

17 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 2.3
5. BladeLogic Operations Manager Version 7.4.2 Security Target *version 2.0, dated 11 November 2009*
6. Evaluation Technical Report For a Target of Evaluation BladeLogic Operations Manager 7.4.2 Security Target v2.0 Evaluation Technical Report v1.0 dated 11 November 2009.