Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ver. 3.1 rel. 5

Certificato n. *(Certificate No.)*	11/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/12/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	19 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	JBoss Enterprise Application Platform (EAP) 8 version 8.1.0.1
Sviluppatore *(Developer)*	Red Hat, Inc.
Tipo di Prodotto *(Type of Product)*	Altre categorie – Application server
Livello di Garanzia *(Assurance Level)*	EAL2+ (ALC_FLR.3) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 19 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

JBoss Enterprise Application Platform (EAP) 8 version 8.1.0.1

OCSI/CERT/ATS/12/2024/RC

Version 1.0

19 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	19/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

API	Application Programming Interface
CM	Configuration Management
DMR	Dynamic Management Representation
EAP	Enterprise Application Platform
EJB	Jakarta Enterprise Beans
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IIOP	Internet Inter-ORB Protocol

JAAS	Java Authentication and Authorization Services
JATAX	Java API for XML Transationing
Jakarta EE	Jakarta Enterprise Edition
JAX-RS	Java API for RESTful Web Services
JAX-WS	Java API for XML Web Services
JDK	Java Development Kit
JMS	Jakarta Messaging Service
JNDI	Java Naming and Directory Interface
LDAP	Lightweight Directory Access Protocol
MSC	Modular Service Container
ORB	Object Request Broker
RBAC	Role-Based Access Control
RMI-IIOP	Remote Method Invocation over Internet Inter-ORB Protocol
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VFS	Virtual File System
XML	Extensible Markup Language

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 5/23 – Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[ETRv.2.1] “JBoss Enterprise Application Platform (EAP) 8 version 8.1” Final Evaluation Technical Report, Evaluation Assurance Level EAL2, augmented by ALC_FLR.3, date 2025-12-24, Version 2.1, atsec information security s.r.l.

[ETRv3] “JBoss Enterprise Application Platform (EAP) 8 version 8.1” Final Evaluation Technical Report, Evaluation Assurance Level EAL2, augmented by ALC_FLR.3, date 2026-02-11, Version 3 atsec information security s.r.l.

[ST] JBoss Enterprise Application Platform Common Criteria Certification 8.1 Security Target– date: 2026-01-30, version 2.0

[JBEAP-CCGUIDE] Red Hat JBoss EAP Common Criteria Certification 8.1 – Common Criteria Configuration Guide
SHA-256:
94492a78087a6c4fb5a6d4a90745272559f8fc8e2f44dc797416f726b0688232
Date 2025-12-23
https://docs.redhat.com/en/documentation/jboss_enterprise_application_platform_common_criteria_certification/8.1/pdf/common_criteria_configuration_guide

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT Products. A higher recognition level for evaluations beyond EAL4 is provided for IT Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product “**JBoss Enterprise Application Platform 8 Version 8.1.0.1**”, developed by Red Hat, Inc.

The TOE is the JBoss Enterprise Application Platform (EAP) which implements an application server. JBoss EAP is based on the Java platform and therefore supports a large variety of operating systems. As an application server, JBoss EAP allows client computers or devices to access applications. Access to these applications is possible through different network protocols, such as HTTP, Remote Method Invocation over Internet Inter-ORB Protocol (RMI-IIOP), and others. JBoss EAP handles the business logic of the application, including accessing and providing the user data required by the application.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3 and NIS5]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should also review the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL2 augmented with ALC_FLR.3, according to the information provided in the Security Target [ST] and in the configuration shown in “Annex B – Evaluated configuration” of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA], and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "JBoss Enterprise Application Platform 8 Version 8.1.0.1" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	JBoss Enterprise Application Platform 8 Version 8.1.0.1
Security Target	JBoss Enterprise Application Platform Common Criteria Certification 8.1, Security Target – date: 2026-01-30, version 2.0 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.3
Developer	Red Hat, Inc.
Sponsor	Red Hat, Inc.
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	1 July 2024
Evaluation ending date	24 December 2025

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description refer to the Security Target [ST].

The TOE of JBoss EAP comprises the following components:

- JBoss EAP 8.1.0.1

The TOE does not include the hardware, firmware, operating system or Java virtual machine used to run the software components.

The TOE is the JBoss Enterprise Application Platform which implements an application server. JBoss EAP is based on the Java platform and therefore supports a large variety of operating systems. As an application server, JBoss EAP allows client computers or devices to access applications. Access to these applications is possible through different network protocols, such as HTTP, RMI-IIOP, and others. JBoss EAP handles the business logic of the application, including accessing and providing the user data required by the application.

The TOE is defined as a stand-alone JBoss EAP instance. If a cluster of JBoss EAP nodes is defined, then the entire cluster is defined as one TOE.

For a detailed description of the TOE, refer to sections 1.3, 1.4 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is the JBoss Enterprise Application Platform and consists of the JBoss Modules framework that instantiates the containers/service. The JBoss Module framework manages the set of pluggable component services which are implemented as Jakarta Managed Beans. This allows assembling different configurations and provides flexibility to tailor the configurations to meet specific requirements.
Figure 1 – TOE architecture shows the interoperation of the different components of JBoss EAP. JBoss EAP consists of a modular framework where the administrator can selectively enable components. JBoss EAP offers compliance with the Jakarta EE 10 specification and offers services beyond Jakarta EE. The following description applies to the Figure 1:

- The hardware together with the operating system executes the Java virtual machine which in turn executes the JBoss Modules framework. This framework provides the foundation on which all JBoss EAP containers perform their tasks.
- Each container implements either a service as specified in Jakarta EE 10 or a service providing additional functionality beyond Jakarta EE 10.
- Applications are executed as part of containers (such as the JAX-RS Web Services container or the EJB container) and may utilize services from other containers.

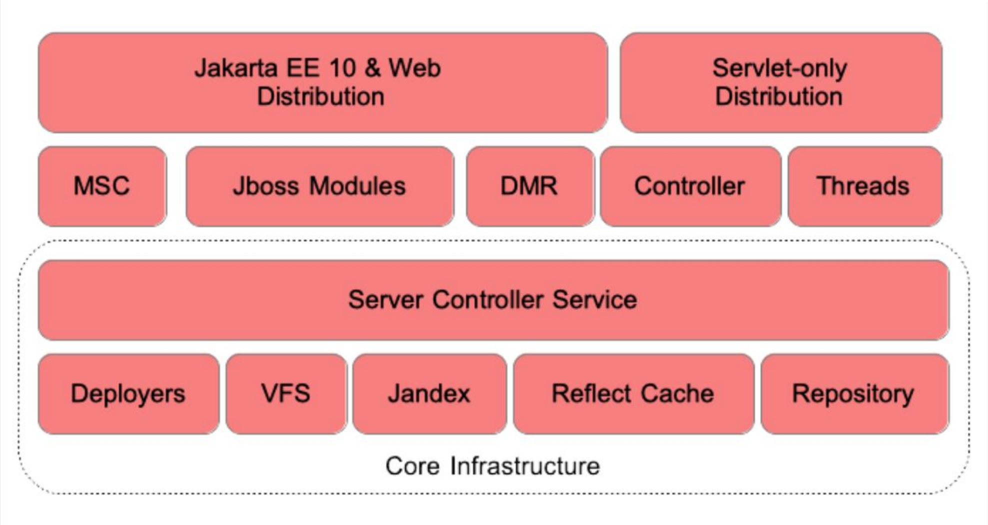

Figure 1 – TOE architecture

The TOE allows interaction with users through the following services:

- HTTP web network protocol.
- RESTful (JAX-RS) and XML-Based (JAX-WS) Web Services.
- Jakarta Enterprise Beans (EJB).
- Jakarta Messaging Service (JMS).
- Java Naming and Directory Interface (JNDI).

Applications utilize the services provided by the different containers by accessing the API exported by each container. These applications are loaded and executed by either the JSP/Servlet container, EJB container or other containers. The technical separation of the untrusted applications and the TOE is achieved using the Java Security Manager with an appropriate policy configuration.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

The major security features of the TOE are:

- Identification and Authentication ensuring the proper identification and authentication of users to facilitate the various access control mechanisms.
- Access Control covering the objects of URLs, EJB methods, message queues and topics.
- Audit covering the access control decisions.
- Clustering ensuring the consistency of user and TSF data between cluster nodes.
- Transaction Rollback ensuring data consistency for user and TSF data.
- Role-based access control to administrative operations and resources.

These primary security features are supported by the appropriate use of domain separation and reference mediation. This separation functionality is provided by the Java virtual machine if the Java Security Manager is utilized. In addition, the underlying operating system supports this separation as well, ensuring that the security features are always invoked and cannot be bypassed, and that the TOE can protect itself.

A detailed description of the TOE security functionality is provided in sections 1.4.4 and 7.1 of the Security Target [ST].

7.4 Documentation

The Common Criteria Guide [JBEAP-CCGUIDE] acts as the main guidance document including the different aspects of the evaluated configuration of the TOE. The Common Criteria Guide can also be downloaded from the Red Hat Customer Portal using the link provided in the bibliographic references. In order to check the integrity of the document, you can execute the command “sha256sum file_name”.

The obtained value must match the SHA-256 hash value:

94492a78087a6c4fb5a6d4a90745272559f8fc8e2f44dc797416f726b0688232.

JBoss Enterprise Application Platform 8.1 documentation includes additional relevant guidance for the secure operation of the TOE that are listed in section 1.5.4.1 of [ST]. In the same section further documentation relevant to JBoss Enterprise Application Platform 7.4, which are applicable to the TOE, are also enlisted. Reference section 8.3 in [ST] reports each document with its SHA-256 hash.

In order to check the integrity of each document, users can execute the command "sha256sum file_name" to verify that the obtained value matches the SHA-256 hash value available in section 8.3 of [ST].

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 2 assurance package, augmented with the CC Part 3 component ALC_FLR.3.

All the SFRs have been selected or derived by extension from CC Part 2 [CC2] (it includes FDP_ROL_EXT.2 as extended component).

Security Target [ST] provides a complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that it constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security s.r.l. The evaluation was completed on 24 December 2025, with the issuance by LVS of the Evaluation Technical Report v2.1 ([ETRv2.1]), which was approved by the Certification Body on February 3rd, 2026. After the conclusion of the evaluation, a new version of the Evaluation Technical Report ([ETRv3]) was issued to reflect few editorial changes in the evaluation documentation and was delivered on 12 February 2026.

Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration".

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report v2.1 [ETRv.2.1] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "JBoss Enterprise Application Platform 8 Version 8.1.0.1" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.3 (augmentations are represented in italics in Table 1).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Systematic Flaw remediation	*ALC_FLR.3*	*Pass*
Test	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass

Assurance classes and components		**Verdict**
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “JBoss Enterprise Application Platform 8 Version 8.1.0.1” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “*Security Objectives for the Operational Environment*” specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.2 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, “Annex A – Guidelines for the secure usage of the product” includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE (Common Criteria Guide [JBEAP-CCGUIDE]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

Section 1.5.4.1 "Physical" of the [ST] provides instructions for the electronic download mechanism and the hash verification for both the TOE JBoss EAP 8.1, and the Common Criteria Guide [JBEAP-CCGUIDE].

The TOE is available at the URL of Red Hat Customer Portal [RHCP] and provided in two ZIP format packages (jboss-eap-8.1.0.zip and jboss-eap-8.1.0.1-maven-repository.zip) and the security administrator must access to the [RHCP] using an account that has a subscription to JBoss Enterprise Application Platform 8 Version 8.1.0.1. Integrity of these packages is ensured by running the following commands and verifying that the SHA-256 hash value provided for each package in the download page matches the value obtained.

```
sha256sum jboss-eap-8.1.0.zip
sha256sum jboss-eap-8.1.0.1-maven-repository.zip
```

The obtained value must match the following SHA-256 hash values:

- jboss-eap-8.1.0.zip:
  - c00ba9f5447a2e6280c0b55f3521052d1b53c18f08eea4acf366e572201f8a2b.
- jboss-eap-8.1.0.1-maven-repository.zip:
  - 8c1fdf0fc5b200b267bb08aee068fa135821a540d5ed1a77eef2621be331395a.

Section 3.4 "ZIP INSTALLATION" and subsection 3.4.1 "Download JBoss EAP" in the Common Criteria Guide [JBEAP-CCGUIDE] shall be followed.

9.2 Installation, configuration, and secure usage of the TOE

TOE installation, configuration and secure usage must be performed following the instructions contained in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria Guide [JBEAP-CCGUIDE] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

The Common Criteria Guide can also be downloaded from the Red Hat Customer Portal [RHCP] using the link provided in the bibliographic references. In order to check the integrity of the document, you can follow the steps available in section 7.4 Documentation.

10 Annex B – Evaluated configuration

The Evaluators have followed the preparation steps for the TOE defined in Common Criteria Guide [JBEAP-CCGUIDE] for the evaluated configuration.

The TOE is JBoss Enterprise Application Platform (EAP) 8 version 8.1.0.1, it is a Java-based application server which provides many advanced product features, including compliance with Jakarta EE 10, clustering, fail-over, and load balancing.

The TOE does not include the hardware, firmware, operating system or Java virtual machine used to run the software components.

JBoss EAP handles the business logic of the application, including accessing and providing the user data required by the application.

The TOE is defined as a stand-alone JBoss EAP instance, if a cluster of JBoss EAP nodes is defined, then the entire cluster is defined as one TOE.

The TOE is supplied via the Red Hat Customer Portal [RHCP] and the security administrator must access to the Red Hat Customer Portal using an account that has a subscription to JBoss Enterprise Application Platform 8 Version 8.1.0.1 (see section 9.1 "TOE delivery").

The items described in section 10.1 "TOE operational environment" must be available before performing the installation.

10.1 TOE operational environment

The Operational Environment for the TOE allows the use of one of the following operating systems, together with one of the associated Java Development Kits (JDK):

- Red Hat Enterprise Linux 8 (x86_64)
  - OpenJDK 17
  - OpenJDK 21
  - Oracle JDK 17
  - Oracle JDK 21
  - Adoptium JDK 17
  - Adoptium JDK 21
- Red Hat Enterprise Linux 9 (x86_64)
  - OpenJDK 17
  - OpenJDK 21
  - Oracle JDK 17
  - Oracle JDK 21
  - Adoptium JDK 17
  - Adoptium JDK 21
- Red Hat Enterprise Linux 10 (x86_64)
  - OpenJDK 17
  - OpenJDK 21
  - Oracle JDK 17
  - Oracle JDK 21
  - Adoptium JDK 17
  - Adoptium JDK 21
- Microsoft Windows Server 2019 (x86_64)
  - OpenJDK 17
  - OpenJDK 21
  - Oracle JDK 17
  - Oracle JDK 21
  - Adoptium JDK 17
  - Adoptium JDK 21
- Microsoft Windows Server 2022 (x86_64)
  - OpenJDK 17
  - OpenJDK 21
  - Oracle JDK 17
  - Oracle JDK 21
  - Adoptium JDK 17
  - Adoptium JDK 21

For providing the cryptographic services supporting the TLS protocol on which the certificate-based authentication relies on, the TOE uses as default the standard cryptographic service providers shipped with the above-mentioned JDK.

Native code in the operational environment, such as libAIO for Red Hat Enterprise Linux, cannot be used in the evaluated configuration.

As the TOE functionality only relies on the correct operation of the Java virtual machine, the TOE can be executed on any operating system that is supported by the respective Java virtual machine. This also means that any hardware supported by the aforementioned operating systems can be used to execute the TOE.

The following relational databases are allowed to be used with the TOE (the listed databases are part of the operational environment and therefore not covered with security claims in the Security Target):

- IBM DB2 Enterprise 12.1
- Oracle 19c RAC
- Oracle 23ai RAC
- MySQL 8.4
- MariaDB 11
- Microsoft SQL Server 2022
- PostgreSQL 17
- EnterpriseDB Advanced Server 17.5
- SAP ASE 16.1

The internal database (H2 DB) is not supported in the evaluated configuration.

The following LDAP servers are allowed to be used with the TOE (they are part of the operational environment and therefore not covered with security claims in the Security Target):

- Microsoft Active Directory 2019
- Microsoft Active Directory 2022
- Red Hat Directory Server 11.9
- Red Hat Directory Server 12.6
- Red Hat Directory Server 13.0

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

All testing activities were carried out remotely from the LVS premises on the test machine hosted at the at the Developer site, Flexential Data Center 5150 McCrimmon Parkway Suite 419 Morrisville, NC 27560, USA.

Test activities were carried out in accordance with the instructions provided by the Italian Certification Body in the Scheme Information Note 5/23 - Conditions for performing tests remotely in Common Criteria evaluations [NIS5].

As part of independent test, the Evaluator installed the TOE using the Common Criteria Guide [JBEAP-CCGUIDE] and product installation documentation. The test cases were prepared as described in the Developer test plan.

Furthermore, the Developer provided six virtual machines to the Evaluator to support the testing activities. Five of these virtual machines (RHEL 8, RHEL 9, RHEL 10, Windows Server 2019, and Windows Server 2022) correspond to the operating systems explicitly identified in the [ST] as supported platforms for the TOE. An additional virtual machine, configured with RHEL 9, was supplied to host the databases used during testing. This machine was specifically employed to run database instances within Podman containers, serving the Windows-based virtual machines during the evaluation.

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly.

The following operating systems were used for testing, together with the corresponding Java Development Kits (JDKs):

- Red Hat Enterprise Linux 8 (x86_64)
  - OpenJDK 17 & 21
  - Oracle JDK 17 & 21
  - Adoptium JDK 17 & 21
- Red Hat Enterprise Linux 9 (x86_64)
  - OpenJDK 17 & 21
  - Oracle JDK 17 & 21
  - Adoptium JDK 17 & 21
- Red Hat Enterprise Linux 10 (x86_64)
  - OpenJDK 17 & 21
  - Oracle JDK 17 & 21
  - Adoptium JDK 17 & 21
- Microsoft Windows Server 2019 (x86_64)
  - OpenJDK 17 & 21
  - Oracle JDK 17 & 21
  - Adoptium JDK 17 & 21
- Microsoft Windows Server 2022 (x86_64)
  - OpenJDK 17 & 21
  - Oracle JDK 17 & 21
  - Adoptium JDK 17 & 21

The Evaluator used these virtual machines to reproduce and execute the Developer's test cases as part of the independent testing activities, ensuring that the results obtained were consistent with those reported by the Developer.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a very detailed testing approach, covering the functionalities of the TOE with integrated testing environment.

The test mapping document provided by the Developer lists the tree of test suites which comprises of test cases which in turn comprise of the test units. This mapping document also provides the ability to trace the individual test unit back to the interfaces that the test unit covers.

The tests are written in Java and are completely automated and available from the Developer. The Evaluator notes that these test cases are developed upstream in conjunction with the JBoss TOE source code. The tests include applications which are loaded onto the TOE as well as user programs which try to access the applications by interfacing with the TOE.

The test cases contain information about the desired/expected behaviors and validate whether the TOE acts according to the expected behavior(s). If the TOE acts as expected, a pass result is returned to the test framework, otherwise, a fail is returned. The test framework records and collects the test results and presents them in human-readable HTML files.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behavior and the properties of the TSF.

11.2.3 Test results

The test results provided by the Developer were generated on the JDK platforms listed above. As described in the testing approach, the test results for all these automated tests are recorded and collected by the framework and written to HTML files.

The actual test results of all Developer’s tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

As part of independent test, the Evaluator installed the TOE using the Common Criteria Guide [JBEAP-CCGUIDE] and product installation documentation. The test cases are prepared as described in the Developer test plan.

Since all interfaces and subsystems are already covered by the Developer's testing, the Evaluator focused on verifying areas that may not have been exhaustively addressed by the Developer.

Given that identification and authentication, as well as access control, are exercised by nearly all Developer test cases, the Evaluator decided to reproduce the complete set of Developer tests. This approach ensures that the testing strategy includes a broad subset of tests engaging as many interfaces as possible.

Because the Developer's test coverage was deemed sufficient, the Evaluator concentrated on test cases that are also relevant for the vulnerability analysis.

Based on these considerations, the Evaluator selected the following test cases and scenarios:

- The Evaluator performed audit-related test cases to verify that, for each event subject to auditing, a corresponding audit record is correctly generated and logged.
- The Developer's test cases verify access control for HTTP GET and POST requests. As the HTTP HEAD request type requires the web server to fully process the operation but return only the response header, the Evaluator performed dedicated tests to verify the enforcement of I&A for HTTP HEAD requests.

11.3.2 Test results

All Developer’s tests were run successfully and the Evaluators verified the correct behavior of the TSFIs and TSFs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluator performed vulnerability analysis and penetration tests activities on a TOE that was installed and configured according to the CC guidance [JBEAP-CCGUIDE].

A search on public vulnerabilities on TOE components have been conducted. The analysis confirmed that there are no public vulnerabilities exploitable with the TOE implementation and configuration.

The Evaluators designed the following attack scenarios:

- HTTP HEAD protection: missing the protection of the HEAD request type
- External modification of JNDI objects: external untrusted entities can access the JNDI service and modify names by external applications
- External read of internal JNDI names: external untrusted entities can read the list of internal JNDI service names to obtain links to sensitive information
- Fuzzing of remote interfaces: malformed, unexpected or out-of-spec inputs sent to specific remote interfaces

The Evaluators could then conclude that the TOE is resistant to a basic attack potential in its intended operational environment. No exploitable or residual vulnerabilities have been identified.