Red Hat JBoss Web Server 3.1

Red Hat JBoss Web Server 3.1 Service Pack 8 Release Notes

For Use with the Red Hat JBoss Web Server 3.1

Last Updated: 2020-03-17

Red Hat JBoss Web Server 3.1 Red Hat JBoss Web Server 3.1 Service Pack 8 Release Notes

For Use with the Red Hat JBoss Web Server 3.1

Legal Notice

Abstract

These release notes contain important information related to the Red Hat JBoss Web Server 3.1 Service Pack 8.

Table of Contents

CHAPTER 1. RED HAT JBOSS WEB SERVER VERSION 3.1 SERVICE PACK 8 3

CHAPTER 2. INSTALLING THE RED HAT JBOSS WEB SERVER 3.1 4

CHAPTER 3. UPGRADING RED HAT JBOSS WEB SERVER USING THIS SERVICE PACK 5

CHAPTER 4. OS/JVM CERTIFICATIONS 6

CHAPTER 5. SECURITY FIXES 7

CHAPTER 6. RESOLVED ISSUES 8

CHAPTER 7. KNOWN ISSUES 9

CHAPTER 8. UPGRADED COMPONENTS 10

CHAPTER 1. RED HAT JBOSS WEB SERVER VERSION 3.1 SERVICE PACK 8

Welcome to the Red Hat JBoss Web Server version 3.1 Service Pack 8 release.

The primary focus of this release is to provide security updates to Red Hat JBoss Web Server version 3.1.

WARNING

As a result of a security vulnerability (CVE-2020-1938), it is recommended that one disable the AJP Connector, if unusued. Otherwise it is recommended to protect the AJP Connector. For full information and steps, see:https://access.redhat.com/solutions/4851251

When using AJP, it is important to ensure it is not exposed to the internet and that it is bound to the proper IP address.

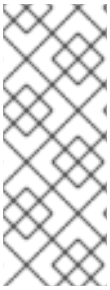
The JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It consists of:

- **Apache Tomcat**: a servlet container in accordance with the Java Servlet Specification. JBoss Web Server contains Apache Tomcat 7 and Apache Tomcat 8.
- The **Apache Tomcat Native Library**: a Tomcat library, which improves Tomcat scalability, performance, and integration with native server technologies.
- The **tomcat-vault extension**: an extension for the JBoss Web Server used for securely storing passwords and other sensitive information used by a JBoss Web Server.
- The **mod_cluster** library: a library that allows communication between Apache Tomcat and the Apache HTTP Server's mod_proxy_cluster module. This allows the Apache HTTP Server to be used as a load balancer for JBoss Web Server.

Service packs for Red Hat JBoss Web Server are produced when a set of critical bug fixes and/or security patches are required before a new full release.

These service pack releases reduce the number of individual patches that we produce and enable customers to keep up to date.

This update includes all fixes and changes from Red Hat JBoss Web Server 3.1 Service Pack 7.



NOTE

From Red Hat JBoss Web Server 3.1 Service Pack 2, all the configuration files that were changed in the patch are appended by the suffix **.zipnew** to avoid overwriting existing configuration files.

If the new or changed properties or configuration options are applicable to you, you will need to manually add or define them in their respective property or configuration file.

CHAPTER 2. INSTALLING THE RED HAT JBOSS WEB SERVER 3.1

The JBoss Web Server 3.1 can be installed using one of the following sections of the installation guide:

- Installing JBoss Web Server on Red Hat Enterprise Linux .
- Installing JBoss Web Server on Microsoft Windows.
- Installing JBoss Web Server on Solaris.

CHAPTER 3. UPGRADING RED HAT JBOSS WEB SERVER USING THIS SERVICE PACK

To install this service pack:

1. Download the Red Hat JBoss Web Server 3.1 Service Pack 8 file (**.zip** format) appropriate to your platform using the download link here (subscription required).

2. Extract the **.zip** file to the Red Hat JBoss Web Server installation directory.

For Red Hat Enterprise Linux users who have installed Red Hat JBoss Web Server from RPM packages, can upgrade to the latest service pack using yum:

```
# yum upgrade
```

CHAPTER 4. OS/JVM CERTIFICATIONS

This update includes no additional certifications.

CHAPTER 5. SECURITY FIXES

This update includes fixes for the following security related issues:

ID	Impact	Summary
CVE-2018-0495	Moderate	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries
CVE-2018-0732	Moderate	openssl: Malicious server can send large prime to client during DH(E) TLS handshake causing the client to hang
CVE-2018-0734	Low	openssl: timing side channel attack in the DSA signature algorithm
CVE-2018-0737	Low	openssl: RSA key generation cache timing vulnerability in crypto/rsa/rsa_gen.c allows attackers to recover private keys
CVE-2019-0221	Low	tomcat: XSS in SSI printenv
CVE-2019-1559	Moderate	openssl: 0-byte record padding oracle
CVE-2019-12418	Moderate	tomcat: local privilege escalation
CVE-2019-17563	Low	tomcat: session fixation when using FORM authentication
CVE-2020-1938	Important	Ghostcat - Apache Tomcat AJP File Read/Inclusion Vulnerability (CNVD-2020-10487)

CHAPTER 6. RESOLVED ISSUES

The following issues are resolved in the current service pack:

Issue	Description
JWS-1527	Use latest JBCS and tomcat-native
JWS-1578	Add rpm changelog entry for CVE-2018-1336

CHAPTER 7. KNOWN ISSUES

The following issues are known in the current service pack release:

Issue	Description
JWS-1583	Update all of the StringManager references back to the original class reference and add the call to getPackage().getName() so that the inits are able to find LocalStrings.properties in the correct packages
Bugzilla Bug-1455483	RFE: Add support for characters "<" and ">" to the possible whitelist values

CHAPTER 8. UPGRADED COMPONENTS

The following components were upgraded in the Red Hat JBoss Web Server 3.1 Service Pack 8 Release:

Component	Version
OpenSSL	1.1.1c
Tomcat-native	1.2.23