



# Red Hat JBoss Web Server 3.1

## Red Hat JBoss Web Server 3.1 Service Pack 14 Release Notes

For Use with the Red Hat JBoss Web Server 3.1



# Red Hat JBoss Web Server 3.1 Red Hat JBoss Web Server 3.1 Service Pack 14 Release Notes

---

For Use with the Red Hat JBoss Web Server 3.1

## Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

These release notes contain important information related to the Red Hat JBoss Web Server 3.1 Service Pack 14.

---

## Table of Contents

CHAPTER 1. RED HAT JBOSS WEB SERVER VERSION 3.1 SERVICE PACK 14 .....	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 14

Welcome to the Red Hat JBoss Web Server version 3.1 Service Pack 14 release. The primary focus of this release is to provide security updates to Red Hat JBoss Web Server version 3.1 (except for Red Hat Enterprise Linux 6 platform as it was discontinued).

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 for Red Hat JBoss Web Server 3.1 Service Pack 12.

This release of Red Hat JBoss Web Server includes some important security updates.



## 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 14 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, you can upgrade to the latest service pack by 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
<a href="#">CVE-2022-23307</a>	Important	log4j: Unsafe deserialization flaw in Chainsaw log viewer [jws-3]
<a href="#">CVE-2022-23305</a>	Important	log4j: SQL injection in Log4j 1.x when application is configured to use JDBCAppender [jws-3]
<a href="#">CVE-2022-23302</a>	Moderate	log4j: Remote code execution in Log4j 1.x when application is configured to use JMSSink [jws-3]
<a href="#">CVE-2021-4104</a>	Moderate	log4j: Remote code execution in Log4j 1.x when application is configured to use JMSAppender [jws-3]

## CHAPTER 6. RESOLVED ISSUES

This release includes the following resolved issue:

Issue	Description
<a href="#">JWS-2377</a>	Update to the latest JBCS released apr and openssl versions

## CHAPTER 7. KNOWN ISSUES

There are no known issues for this release.

## CHAPTER 8. UPGRADED COMPONENTS

There are no upgraded components for this release.