



Red Hat JBoss Core Services 2.4.29

Red Hat JBoss Core Services 2.4.29 Service Pack 1 Release Notes

For Use with the Red Hat JBoss Core Services 2.4.29

Red Hat JBoss Core Services 2.4.29 Red Hat JBoss Core Services 2.4.29 Service Pack 1 Release Notes

For Use with the Red Hat JBoss Core Services 2.4.29

Legal Notice

Copyright © 2019 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, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

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

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

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

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

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

The OpenStack ® 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 Core Services 2.4.29 Service Pack 1.

Table of Contents

CHAPTER 1. RED HAT JBOSS CORE SERVICES 2.4.29 SERVICE PACK 1	3
CHAPTER 2. NEW INSTALLATION OF RED HAT JBOSS CORE SERVICES 2.4.29	4
CHAPTER 3. UPGRADING RED HAT JBOSS CORE SERVICES USING THIS SERVICE PACK	5
CHAPTER 4. SECURITY FIXES	6
CHAPTER 5. RESOLVED ISSUES	8
CHAPTER 6. KNOWN ISSUES	9
CHAPTER 7. UPGRADED COMPONENTS	10

CHAPTER 1. RED HAT JBOSS CORE SERVICES 2.4.29 SERVICE PACK 1

Red Hat JBoss Core Services Apache HTTP Server 2.4.29 Service Pack 1 for RHEL 7 x86_64

Service packs for Red Hat JBoss Core Services 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.

CHAPTER 2. NEW INSTALLATION OF RED HAT JBOSS CORE SERVICES 2.4.29

You may install the Red Hat JBoss Core Services 2.4.29 version using the instructions provided below:

[Installing Apache HTTP Server](#)

Make sure you upgrade to the latest service pack after installing.

CHAPTER 3. UPGRADING RED HAT JBOSS CORE SERVICES USING THIS SERVICE PACK

Download the Red Hat JBoss Core Services 2.4.29 Service Pack 1 file (.zip format) appropriate to your platform using the download link [here \(subscription required\)](#). Extract the .zip file to the Red Hat JBoss Core Services installation directory.

CHAPTER 4. SECURITY FIXES

This update includes fixes for the following security related issues:

ID	Impact	Summary
CVE-2017-10140	Moderate	libdb: Reads DB_CONFIG from the current working directory
CVE-2017-15710	Low	httpd: Out of bounds write in mod_authnz_ldap when using too small Accept-Language values
CVE-2017-15715	Low	httpd: bypass with a trailing newline in the file name
CVE-2018-0739	Moderate	openssl: Handling of crafted recursive ASN.1 structures can cause a stack overflow and resulting denial of service
CVE-2018-1283	Moderate	httpd: Improper handling of headers in mod_session can allow a remote user to modify session data for CGI applications
CVE-2018-1301	Low	httpd: Out of bounds access after failure in reading the HTTP request
CVE-2018-1302	Low	httpd: Use-after-free on HTTP/2 stream shutdown
CVE-2018-1303	Moderate	httpd: Out of bounds read in mod_cache_socache can allow a remote attacker to cause DoS
CVE-2018-1312	Low	httpd: Weak Digest auth nonce generation in mod_auth_digest
CVE-2018-1333	Moderate	httpd: mod_http2: Too much time allocated to workers, possibly leading to DoS
CVE-2018-11759	Important	mod_jk: connector path traversal due to mishandled HTTP requests in httpd

ID	Impact	Summary
CVE-2018-11763	Moderate	httpd: DoS for HTTP/2 connections by continuous SETTINGS frames
CVE-2018-1000168	Moderate	nghttp2: Null pointer dereference when too large ALTSVC frame is received

CHAPTER 5. RESOLVED ISSUES

See the JBoss Developer bug tracking software for a list of the [Resolved issues for Red Hat JBoss Core Services 2.4.29 Service Pack 1](#).

CHAPTER 6. KNOWN ISSUES

See the JBoss Developer bug tracking software for a list of the [Resolved issues for Red Hat JBoss Core Services 2.4.29 Service Pack 1](#).

CHAPTER 7. UPGRADED COMPONENTS

Component	Version	Comment
Mod_jk	1.2.46	Previously 1.2.43