Red Hat JBoss Core Services 2.4.37

Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 3 Release Notes

For Use with the Red Hat JBoss Core Services Apache HTTP Server 2.4.37

Last Updated: 2022-10-20

Red Hat JBoss Core Services 2.4.37 Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 3 Release Notes

For Use with the Red Hat JBoss Core Services Apache HTTP Server 2.4.37

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 ® 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 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 Apache HTTP Server 2.4.37.

Table of Contents

PREFACE

Welcome to the Red Hat JBoss Core Services version 2.4.37 Service Pack 3 release.

Red Hat JBoss Core Services Apache HTTP Server is an open source web server developed by the Apache Software Foundation. Features of Apache HTTP Server include:

- Implements the current HTTP standards, including HTTP/1.1 and HTTP/2.
- Transport Layer Security (TLS) encryption support though OpenSSL, providing secure connections between the web server and web clients.
- Extendable though modules, some of which are included with the Red Hat JBoss Core Services Apache HTTP Server.

CHAPTER 1. INSTALLING THE RED HAT JBOSS CORE SERVICES 2.4.37

The Apache HTTP Server 2.4.37 can be installed using one of the following sections of the installation guide:

- For installation instructions for Red Hat Enterprise Linux systems, see:
  - Installing JBoss Core Services Apache HTTP Server on Red Hat Enterprise Linux: Installation using .zip archives.
  - Installing JBoss Core Services Apache HTTP Server on Red Hat Enterprise Linux: Installation using RPM packages.
- For installation instructions for Microsoft Windows systems, see: Installing JBoss Core Services Apache HTTP Server on Microsoft Windows.

CHAPTER 2. UPGRADING TO THE RED HAT JBOSS CORE SERVICES APACHE HTTP SERVER 2.4.37

NOTE

Where a Red Hat JBoss Core Services Apache HTTP Server 2.4.29 or earlier was installed from RPMs packages using **yum**, the Apache HTTP Server can be upgraded with **yum upgrade**.

For systems where an earlier version of the Red Hat JBoss Core Services Apache HTTP Server was installed from a .zip archive, upgrading to the Apache HTTP Server 2.4.37 Service Pack 3 requires:

1. Installing the Apache HTTP Server 2.4.37.
2. Setting up the Apache HTTP Server 2.4.37.
3. Removing the earlier version of Apache HTTP Server.

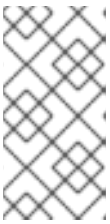
Prerequisites

- Root user access (Red Hat Enterprise Linux systems)
- Administrative access (Windows Server)
- A system where the Red Hat JBoss Core Services Apache HTTP Server 2.4.29 or earlier was installed from a .zip archive.

Procedure

For systems using the Red Hat JBoss Core Services Apache HTTP Server 2.4.29, the recommended procedure for upgrading to the Apache HTTP Server 2.4.37 is:

1. Shutdown any running instances of Red Hat JBoss Core Services Apache HTTP Server 2.4.29.
2. Backup the Red Hat JBoss Core Services Apache HTTP Server 2.4.29 installation and configuration files.
3. Install the Red Hat JBoss Core Services Apache HTTP Server 2.4.37 using the .zip installation method for the current system (see Additional Resources below).
4. Migrate your configuration from the Red Hat JBoss Core Services Apache HTTP Server version 2.4.29 to version 2.4.37.



NOTE

The Apache HTTP Server configuration files may have changed since the Apache HTTP Server 2.4.29 release. It is recommended that you update the 2.4.37 version configuration files, rather than overwrite them with the configuration files from a different version (such as the Apache HTTP Server 2.4.29).

5. Remove the Red Hat JBoss Core Services Apache HTTP Server 2.4.29 root directory.

Additional Resources

- For installation instructions for Red Hat Enterprise Linux systems, see:

- Installing JBoss Core Services Apache HTTP Server on Red Hat Enterprise Linux: Installation using .zip archives.
- Installing JBoss Core Services Apache HTTP Server on Red Hat Enterprise Linux: Installation using RPM packages.

- Installing JBoss Core Services Apache HTTP Server on Microsoft Windows .

CHAPTER 3. SECURITY FIXES

This update includes fixes for the following security related issues:

ID	Impact	Summary
CVE-2018-20843	Moderate	expat: large number of colons in input makes parser consume high amount of resources, leading to DoS
CVE-2019-0196	Low	httpd: mod_http2: read-after-free on a string compare
CVE-2019-0197	Low	httpd: mod_http2: possible crash on late upgrade
CVE-2019-15903	Low	expat: heap-based buffer over-read via crafted XML input
CVE-2019-19956	Moderate	libxml2: There's a memory leak in xmlParseBalancedChunkMemory Recover in parser.c that could result in a crash
CVE-2019-20388	Moderate	libxml2: memory leak in xmlSchemaPreRun in xmlschemas.c
CVE-2020-1934	Low	httpd: mod_proxy_ftp use of uninitialized value
CVE-2020-7595	Moderate	libxml2: infinite loop in xmlStringLenDecodeEntities in some end-of-file situations
CVE-2020-11080	Important	nghttp2: overly large SETTINGS frames can lead to DoS

CHAPTER 4. RESOLVED ISSUES

The following are resolved issues for this release:

Issue	Summary
JBCS-257	graceful start failure due to wrong path to /sbin/apachectl
JBCS-425	Mod_cluster EnableWsTunnel enables only ws comunication
JBCS-495	Update references to 'the Apache HTTP'
JBCS-501	Change instances of ZIP
JBCS-529	Documentation for mod_security
JBCS-651	mod_cluster does not properly disable session stickiness
JBCS-761	Documentation error in naming jbcs-httpd2.4-httpd-selinux
JBCS-884	Empty directories used by caching are still present on File System even after specifying "-t" to delete them with htcacheclean
JBCS-929	Automatic resolution of JBCS_HOME in apxs
JBCS-931	Rebase mod_http2 to 1.15.7
JBCS-933	fix health check for wss
JBCS-935	cannot override default Virtualhost's mod_reqtimeout
JBCS-936	**Tech Preview:** Add openssl-pkcs11 to JBCS
JBCS-941	Upgrade mod_cluster native to 1.3.14
JBCS-946	Setting smax results in very small max connection pool on mod_cluster
JBCS-948	Upgrade mod_jk to 1.2.48
JBCS-949	Update libxml2 to use gerrit lookaside and sync with rhel-8.3.0

CHAPTER 5. KNOWN ISSUES

The following are known issues for this release:

Issue	Summary
JBCS-589	The mod_jk module needs more detailed documentation
JBCS-621	Provide brief overview of the difference between Apache HTTPD on RHEL and JBCS Apache HTTP
JBCS-838	Installation steps to upgrade 2.4.29 SP2 from 2.4.29 should be described.
JBCS-940	ModJK and ModCluster Documentation: adding how to configure their respective secret directive

CHAPTER 6. UPGRADED COMPONENTS

This release includes upgraded versions of the following packages:

Component	Version	Operating Systems
mod_jk	1.2.48	All
mod_cluster native	1.3.14	All
mod_http2	1.15.7	All
openssl-pkcs11	0.4.10	RHEL 7 and Windows