



Red Hat JBoss Core Services 2.4.29

Red Hat JBoss Core Services Apache HTTP Server 2.4.29 Service Pack 2 Release Notes

For Use with the Red Hat JBoss Core Services Apache HTTP Server 2.4.29

Red Hat JBoss Core Services 2.4.29 Red Hat JBoss Core Services Apache HTTP Server 2.4.29 Service Pack 2 Release Notes

For Use with the Red Hat JBoss Core Services Apache HTTP Server 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, 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 2.4.29.

Table of Contents

PREFACE	3
CHAPTER 1. INSTALLING THE RED HAT JBOSS CORE SERVICES 2.4.29 SERVICE PACK 2	4
CHAPTER 2. UPGRADING TO THE RED HAT JBOSS CORE SERVICES APACHE HTTP SERVER 2.4.29	5
Prerequisites	5
Procedure	5
Additional Resources	5
CHAPTER 3. SECURITY FIXES	7
CHAPTER 4. RESOLVED ISSUES	8
CHAPTER 5. KNOWN ISSUES	9
CHAPTER 6. UPGRADED COMPONENTS	10

PREFACE

Welcome to the Red Hat JBoss Core Services version 2.4.29 Service Pack 2 release.

This release of Red Hat JBoss Core Services focuses on updates for RHEL 6 and 7. It also covers several security issues as well.

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 through [OpenSSL](#), providing secure connections between the web server and web clients.
- Extendable through 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 2.4.29 SERVICE PACK 2

The Apache HTTP Server 2.4.29 Service Pack 2 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.](#)
- For installation instructions for Solaris systems, see: [Installing Apache HTTP Server on Solaris .](#)

CHAPTER 2. UPGRADING TO THE RED HAT JBOSS CORE SERVICES APACHE HTTP SERVER 2.4.29



NOTE

Where a Red Hat JBoss Core Services Apache HTTP Server 2.4.23 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 2.4.29 Service Pack 2 requires:

1. Installing the Apache HTTP Server 2.4.29.
2. Setting up the Apache HTTP Server 2.4.29.
3. Removing the earlier version of Apache HTTP Server.

Prerequisites

- Root user access (Red Hat Enterprise Linux and Solaris systems)
- Administrative access (Windows Server)
- A system where the Red Hat JBoss Core Services Apache HTTP Server 2.4.23 or earlier was installed from a .zip archive.

Procedure

For systems using the Red Hat JBoss Core Services Apache HTTP Server 2.4.23, the recommended procedure for upgrading to the Apache HTTP Server 2.4.29 is:

1. Shutdown any running instances of Red Hat JBoss Core Services Apache HTTP Server 2.4.23.
2. Backup the Red Hat JBoss Core Services Apache HTTP Server 2.4.23 installation and configuration files.
3. Install the Red Hat JBoss Core Services Apache HTTP Server 2.4.29 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 2.4.23 to version 2.4.29.



NOTE

The Apache HTTP Server configuration files may have changed since the Apache HTTP Server 2.4.23 release. It is recommended that you update the 2.4.29 version configuration files, rather than overwrite them with the configuration files from a different version (such as Apache HTTP Server 2.4.23).

5. Remove the Red Hat JBoss Core Services Apache HTTP Server 2.4.23 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.](#)
- For installation instructions for Microsoft Windows systems, see: [Installing JBoss Core Services Apache HTTP Server on Microsoft Windows.](#)
- For installation instructions for Solaris systems, see: [Installing Apache HTTP Server on Solaris .](#)

CHAPTER 3. SECURITY FIXES

This update includes fixes for the following security related issues:

ID	Impact	Summary
CVE-2018-0495	Moderate	openssl: 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-2018-14404	Moderate	libxml2: NULL pointer dereference in xpath.c:xmlXPathCompOpEval() can allow attackers to cause a denial of service
CVE-2018-16890	Moderate	curl: NTLM type-2 heap out-of-bounds buffer read
CVE-2018-1000005	Low	curl: Out-of-bounds read in code handling HTTP/2 trailers
CVE-2018-1000007	Moderate	curl: HTTP authentication leak in redirects
CVE-2018-1000120	Moderate	curl: FTP path trickery leads to NIL byte out of bounds write
CVE-2018-1000122	Moderate	curl: RTSP RTP buffer over-read
CVE-2019-0211	Important	httpd: privilege escalation from modules scripts
CVE-2019-3822	Moderate	curl: NTLMv2 type-3 header stack buffer overflow
CVE-2019-3823	Low	curl: SMTP end-of-response out-of-bounds read

CHAPTER 4. RESOLVED ISSUES

The following are non-security issues resolved during this release:

Issue	Description
JBCS-620	httpd segfaults when doing graceful reload
JBCS-750	httpd segfaults when doing graceful reload
JBCS-722	Rebase to curl 7.64.1

CHAPTER 5. KNOWN ISSUES

There are currently no known issues for this release

CHAPTER 6. UPGRADED COMPONENTS

This release does not include any updates to its components.