Red Hat JBoss Core Services 2.4.37

Red Hat JBoss Core Services Apache HTTP Server 2.4.37 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 Release Notes

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

Legal Notice

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 release.

IMPORTANT

This version of JBCS will be dropping support for Solaris systems. JBCS will continue to support both RHEL and Windows systems, but all support for Solaris has been dropped from this update.

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 {SP-0} 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-2018-0734	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-2018-17189	Low	mod_http2: DoS via slow, unneeded request bodies
CVE-2018-17199	Moderate	mod_session_cookie does not respect expiry time
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-2019-0217	Moderate	httpd: mod_auth_digest: access control bypass due to race condition [jbcs-httpd-2.4.29]
CVE-2019-9511	Important	large amount of data requests leads to denial of service
CVE-2019-9513	Important	flood using PRIORITY frames results in excessive resource consumption
CVE-2019-9516	Important	HTTP/2: 0-length headers lead to denial of service
CVE-2019-9517	Important	HTTP/2: request for large response leads to denial of service

CHAPTER 4. RESOLVED ISSUES

The following are resolved issues for this release:

Issue	Summary
JBCS-163	jbcs-httpd24-openssl-perl depends on perl(WWW::Curl::Easy) from base-os optional
JBCS-255	Backport DeflateAlterETag directive to httpd 2.4
JBCS-315	Typo in comment of sample configuration
JBCS-399	stickysession parameter specified in ProxyPass line is not enabled
JBCS-448	mod_proxy_hcheck should be aware of BalancerMember's connectiontimeout parameter and should timeout based on it
JBCS-590	APR zip does not contain docs
JBCS-634	High CPU in mod_cluster with high httpd VirtualHost counts when restarting JBoss instances
JBCS-685	Provide OpenSSL which includes TLS 1.3 support (once at upstream available) as a part of JBCS
JBCS-695	Apache httpd with worker/event mpm segfaults after multiple successive graceful reloads triggered by logrotate
JBCS-710	Failover scenario is not performed with httpd balancer - balancer fails to respond
JBCS-715	Missing doc and src zips
JBCS-717	Impossible to disable insertion of header=expect=100-Continue in proxied requests
JBCS-729	mod_cluster routing mix up after upgrade to 2.4.29
JBCS-740	JON Apache plugin fails to discover JBCS Apache HTTP with SP1 applied
JBCS-748	JWS3.0-Optional rpms in the EWS installation guide for httpd zip
JBCS-788	Drop mod_rt and mod_bmx

Issue	Summary
JBCS-794	Change in LICENSE file
JBCS-798	Segfault when DeterministicFailover On
JBCS-801	Drop mod_auth_kerb
JBCS-809	Mod_speling is not enabled by default

CHAPTER 5. KNOWN ISSUES

There are no known issues for this release.

CHAPTER 6. UPGRADED COMPONENTS

This release includes upgraded versions of the following packages:

Component	Version	Operating Systems
curl	7.64.1	Microsoft Windows and RHEL
openssl	1.1.1	Microsoft Windows and RHEL
Mod_Cluster	1.3.12.Final	Microsoft Windows and RHEL
Mod_jk	1.2.46	Microsoft Windows and RHEL