Red Hat JBoss Core Services 2.4.37

Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 8 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 8 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 Service Pack 8 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.

IMPORTANT

Red Hat Enterprise Linux 6 is no longer supported and subsequently was removed from the documentation.

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

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 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

- 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. Shut down any running instances of Red Hat JBoss Core Services Apache HTTP Server 2.4.29.
2. Back up 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

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

CHAPTER 3. SECURITY FIXES

This update includes the following security fixes:

ID	Impact	Summary
CVE-2020-8284	Moderate	curl: FTP PASV command response can cause curl to connect to arbitrary host [jbcs-httpd-2.4]
CVE-2020-8286	Moderate	curl: inferior OCSP verification [jbcs-httpd-2.4]
CVE-2020-8169	Moderate	curl: libcurl: partial password leak over DNS on HTTP redirect [jbcs-httpd-2.4]
CVE-2021-22876	Moderate	curl: Leak of authentication credentials in URL via automatic Referer [jbcs-httpd-2.4]
CVE-2020-8285	Moderate	curl:malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is used [jbcs-httpd-2.4]
CVE-2021-22890	Low	curl: TLS 1.3 session ticket mix-up with HTTPS proxy host [jbcs-httpd-2.4]
CVE-2021-22901	Important	curl: Use-after-free in TLS session handling when using OpenSSL TLS backend [jbcs-httpd-2.4]
CVE-2021-31618	Important	httpd: NULL pointer dereference on specially crafted HTTP/2 request [jbcs-httpd-2.4]

CHAPTER 4. RESOLVED ISSUES

The following are resolved issues for this release:

Issue	Summary
JBCS-1100	mod_cluster never removes hung JVM that has requests routed to it.
JBCS-1131	HTTP 400 error for FQDN/URL with more than 14 character
JBCS-1075	HTTP/1.1 is broken with using WebSockets (and mod_cluster) in SP6
JBCS-1111	/opt/rh/jbcs-httpd24/root/usr/sbin/apx looks broken... missing deps

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	7.77.0	Windows
libcurl	7.77.0	RHEL 7 & RHEL 8