Red Hat JBoss Core Services 2.4.37

Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 10 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 10 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 10 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.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our technical content and encourage you to tell us what you think. If you'd like to add comments, provide insights, correct a typo, or even ask a question, you can do so directly in the documentation.

NOTE

You must have a Red Hat account and be logged in to the customer portal.

To submit documentation feedback from the customer portal, do the following:

1. Select the **Multi-page HTML** format.
2. Click the **Feedback** button at the top-right of the document.
3. Highlight the section of text where you want to provide feedback.
4. Click the **Add Feedback** dialog next to your highlighted text.
5. Enter your feedback in the text box on the right of the page and then click **Submit**.

We automatically create a tracking issue each time you submit feedback. Open the link that is displayed after you click **Submit** and start watching the issue or add more comments.

Thank you for the valuable feedback.

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

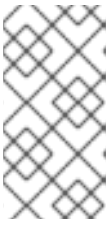
Prerequisites

- 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-2021-41773	Important	httpd: path traversal and file disclosure vulnerability [jbcs-httpd-2.4]
CVE-2021-40438	Important	httpd: mod_proxy: SSRF via a crafted request uri-path containing "unix:" [jbcs-httpd-2.4]
CVE-2021-3712	Moderate	openssl: Read buffer overruns processing ASN.1 strings [jbcs-httpd-2.4]
CVE-2021-3688	Moderate	mod_proxy: Red Hat JBCS: URL normalization issue with dot-dot-semicolon(s) leads to information disclosure [jbcs-httpd-2.4]
CVE-2021-22924	Moderate	curl: Bad connection reuse due to flawed path name checks [jbcs-httpd-2.4]
CVE-2021-22922	Moderate	curl: Content not matching hash in Metalink is not being discarded [jbcs-httpd-2.4]
CVE-2021-22923	Moderate	curl: Metalink download sends credentials [jbcs-httpd-2.4]
CVE-2021-30641	Moderate	httpd: Unexpected URL matching with 'MergeSlashes OFF' [jbcs-httpd-2.4]
CVE-2019-17567	Moderate	httpd: mod_proxy_wstunnel tunneling of non Upgraded connection [jbcs-httpd-2.4]
CVE-2021-26691	Moderate	httpd: mod_session: Heap overflow via a crafted SessionHeader value [jbcs-httpd-2.4]
CVE-2021-26690	Moderate	httpd: mod_session: NULL pointer dereference when parsing Cookie header [jbcs-httpd-2.4]

ID	Impact	Summary
CVE-2021-23840	Moderate	openssl: integer overflow in CipherUpdate [jbcs-httpd-2.4]
CVE-2021-23841	Moderate	openssl: NULL pointer dereference in X509_issuer_and_serial_hash() [jbcs-httpd-2.4]
CVE-2020-14155	Low	pcre: Integer overflow when parsing callout numeric arguments [jbcs-httpd-2.4]
CVE-2019-20838	Low	pcre: Buffer over-read in JIT when UTF is disabled and \X or \R has fixed quantifier greater than 1 [jbcs-httpd-2.4]
CVE-2021-22925	Low	curl: Incorrect fix for CVE-2021-22898 TELNET stack contents disclosure [jbcs-httpd-2.4]
CVE-2020-13950	Low	httpd: mod_proxy NULL pointer dereference [jbcs-httpd-2.4]
CVE-2020-35452	Low	httpd: Single zero byte stack overflow in mod_auth_digest [jbcs-httpd-2.4]

CHAPTER 4. RESOLVED ISSUES

The following are resolved issues for this release:

Issue	Summary
JBCS-1225	Add fix for CVE-2021-41773
JBCS-1186	[GSS] Segmentation fault in ap_increment_counts
JBCS-1177	Rebase curl to 7.78.0
JBCS-1152	Segmentation fault during string tokenization
JBCS-1149	SSLProtocol with based virtual hosts
JBCS-1147	mod_proxy_http fills file system with /tmp/modproxy.tmp.* files
JBCS-1074	prunsrv stop timeout not honored
JBCS-985	Upgrade Apache Commons Daemon JSVC (for Windows) to version 1.2.4
JBCS-957	JBoss Service.bat stop fails with an error

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
apache-commons-daemon-jsvc	1.2.4	Microsoft Windows
curl	7.78.0	Microsoft Windows

For a full list of components that are supported in this release of Red Hat JBoss Core Services, see the Core Services Apache HTTP Server Component Details page. Before you attempt to access the Component Details page, you must ensure that you have an active Red Hat subscription and you are logged in to the Red Hat Customer Portal.