Red Hat JBoss Core Services 2.4.23

Apache HTTP Server 2.4.23 Release Notes

For use with Red Hat JBoss middleware products.

Last Updated: 2018-05-23

Red Hat JBoss Core Services 2.4.23 Apache HTTP Server 2.4.23 Release Notes

For use with Red Hat JBoss middleware products.

Legal Notice

Abstract

These release notes contain important information related to Red Hat JBoss Core Services.

Table of Contents

CHAPTER 1. INTRODUCTION TO RED HAT JBOSS CORE SERVICES

1.1. ABOUT RED HAT JBOSS CORE SERVICES

Red Hat JBoss Core Services is a set of supplementary software for Red Hat JBoss middleware products. This software, such as Apache HTTP Server, is common to multiple JBoss middleware products, and is packaged under Red Hat JBoss Core Services to allow for faster distribution of updates, and for a more consistent update experience.

1.2. ABOUT JBOSS CORE SERVICES APACHE HTTP SERVER

Apache HTTP Server is used in multiple Red Hat JBoss middleware products, and previously Apache HTTP Server was distributed with each JBoss product. Starting from the following product versions, each product will instead use the JBoss Core Services distribution of Apache HTTP Server:

- Red Hat JBoss Core Services (Apache HTTP Server) 7.0 and onwards.

IMPORTANT

The Apache HTTP Server distribution included as part of Red Hat Enterprise Linux is completely separate from the JBoss Core Services distribution of Apache HTTP Server.

1.3. SUPPORTED OPERATING SYSTEMS AND CONFIGURATIONS

For information on supported operating systems and configurations for JBoss Core Services Apache HTTP Server, see https://access.redhat.com/articles/2258971.

CHAPTER 2. NEW FEATURES AND ENHANCEMENTS

2.1. HTTP/2.0 SUPPORT

JBoss Core Services now includes **`mod_http2`**, providing HTTP/2.0 features which have been tested under a TLS configuration. This protocol features HTTP header compression, and allows the server to preemptively provide data it thinks will be needed to the client, reducing the time needed to fully load pages.

2.2. APACHE HTTP SERVER UPGRADE

The Apache HTTP server has been upgraded to 2.4.23.

2.3. OPENSSL UPGRADE

OpenSSL has been updated to 1.0.2h.

CHAPTER 3. VERIFIED AND RESOLVED CVES

3.1. VERIFIED CVES

The following CVEs have been verified in this release:

CVE-2012-1148

A memory-leak flaw was found in Expat. If an XML file processed by an application linked against Expat triggered a memory re-allocation failure, Expat failed to free the previously allocated memory. This could cause the application to exit unexpectedly or crash when all available memory was exhausted.

CVE-2014-3523

A memory leak was found in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the httpd on Windows. When the default AcceptFilter was enabled, this allowed remote attackers to cause a denial of service (memory consumption) using crafted requests.

CVE-2014-8176

An invalid-free flaw was found in the way OpenSSL handled certain DTLS handshake messages. A malicious DTLS client or server could send a specially crafted message to the peer, which could then cause the application to crash or potentially result in arbitrary code execution.

CVE-2016-1834

A heap-based buffer overflow vulnerability in the xmlStrncat function in libxml2 allowed remote attackers to execute arbitrary code or cause a denial of service (memory corruption) using a crafted XML document.

CVE-2016-1840

A heap-based buffer overflow vulnerability was found in the xmlFAParsePosCharGroup function in libxml2. The flaw allowed remote attackers to execute arbitrary code or cause a denial of service (memory corruption) using a crafted XML document.

CVE-2016-2108

A flaw was found in the way OpenSSL encoded certain ASN.1 data structures. An attacker could use this flaw to create a specially crafted certificate which, when verified or re-encoded by OpenSSL, could cause it to crash, or execute arbitrary code using the permissions of the user running an application compiled against the OpenSSL library.

CVE-2016-4459

A buffer-overflow vulnerability was discovered in mod_cluster. When using a JVMRoute path longer than 80 characters in the configuration, a segmentation fault occurred leading to a server crash.

CVE-2016-6808

A buffer-overflow vulnerability was discovered in mod_jk, where the virtual host name and the URI are concatenated to create a virtual host mapping rule. It was found that the length checks prior to writing to the target buffer for this rule did not take into account the length of the virtual host name, creating the potential for a buffer overflow.

CVE-2016-8612

A protocol-parsing flaw was found in mod_cluster’s load balancer, which allowed an attacker to cause a segmentation fault.

CVE-2016-2178

It was discovered that OpenSSL did not always use constant time operations when computing Digital Signature Algorithm (DSA) signatures. A local attacker could possibly use this flaw to obtain a private DSA key belonging to another user or service running on the same system.

CVE-2016-2177

Multiple integer-overflow flaws were found in the way OpenSSL performed pointer arithmetic. A remote attacker could possibly use these flaws to cause a TLS/SSL server or client using OpenSSL to crash.

3.2. RESOLVED CVES

The following CVEs have been included in this release, but have yet to be functionally tested:

CVE-2015-0286

An invalid pointer use flaw was found in OpenSSL's ASN1_TYPE_cmp() function. With a specially crafted X.509 certificate that had been verified by the application, a remote attacker could crash a TLS/SSL client or server using OpenSSL.

CVE-2015-3196

A race-condition flaw, leading to a double-free vulnerability, was found in the way OpenSSL handled pre-shared key (PSK) identify hints. A remote attacker could use this flaw to crash a multi-threaded SSL/TLS client using OpenSSL.

CVE-2016-5419

It was found that the libcurl library did not prevent TLS session resumption after the client certificate had changed. An attacker could potentially use this flaw to hijack connection authentication by leveraging a previously created connection with a different client certificate.

CVE-2016-5420

It was found that the libcurl library did not check the client certificate when choosing the TLS connection to reuse. An attacker could potentially use this flaw to hijack connection authentication by leveraging a previously created connection with a different client certificate.

CVE-2016-0799

Several flaws were found in the way BIO_*printf functions were implemented in OpenSSL. Applications which passed large amounts of untrusted data through these functions could crash or potentially execute code with the permissions of the user running such an application.

CVE-2016-2842

Several flaws were found in the way BIO_*printf functions were implemented in OpenSSL. Applications which passed large amounts of untrusted data through these functions could crash or potentially execute code with the permissions of the user running such an application.

CVE-2016-7141

It was found that, in certain cases, the libcurl library using the NSS (Network Security Services) library as its TLS/SSL backend incorrectly reused client certificates for subsequent TLS connections. An attacker could potentially use this flaw to hijack connection authentication by leveraging a previously created connection with a different client certificate.

CVE-2016-1838

The xmlParserPrintFileContextInternal function in libxml2 allowed remote attackers to cause a denial of service (heap-based buffer over-read) using a crafted XML document.

CVE-2016-1762

The xmlNextChar function in libxml2 before 2.9.4 allowed remote attackers to cause a denial of service (heap-based buffer over-read) using a crafted XML document.

CVE-2016-1837

Multiple use-after-free vulnerabilities were found in the htmlParsePubidLiteral and htmlParseSystemiteral functions in libxml2 that allowed remote attackers to cause a denial of service using a crafted XML document.

CVE-2016-1833

The htmlCurrentChar function in libxml2 allowed remote attackers to cause a denial of service (heap-based buffer over-read) using a crafted XML document.

CVE-2016-4447

The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allowed context-dependent attackers to cause a denial of service (heap-based buffer under-read and application crash) using a crafted file, involving xmlParseName.

CVE-2016-1835

A use-after-free vulnerability was found in the xmlSAX2AttributeNs function in libxml2 that allowed remote attackers to cause a denial of service using a crafted XML document.

CVE-2016-4449

An XML external entity (XXE) vulnerability was found in the xmlStringLenDecodeEntities function in parser.c in libxml2 , when not in validating mode, which could allow context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) using unspecified vectors.

CVE-2016-1839

The xmlDictAddString function in libxml2 allowed remote attackers to cause a denial of service (heap-based buffer over-read) using a crafted XML document.

CVE-2016-1836

A use-after-free vulnerability was found in the xmlDictComputeFastKey function in libxml2 that allowed remote attackers to cause a denial of service using a crafted XML document.

CVE-2016-4448

A format-string vulnerability in libxml2 allowed attackers to have an unspecified impact using format string specifiers in unknown vectors.

CVE-2016-2107

It was discovered that OpenSSL leaked timing information when decrypting TLS/SSL and DTLS protocol encrypted records when the connection used the AES CBC cipher suite and the server supported AES-NI. A remote attacker could possibly use this flaw to retrieve plain text from encrypted packets by using a TLS/SSL or DTLS server as a padding oracle.

CVE-2016-2106

An integer-overflow flaw, leading to a buffer overflow, was found in the way the EVP_EncryptUpdate() function of OpenSSL parsed very large amounts of input data. A remote attacker could use this flaw to crash an application using OpenSSL or, possibly, execute arbitrary code with the permissions of the user running that application.

CVE-2016-2105

An integer-overflow flaw, leading to a buffer overflow, was found in the way the EVP_EncodeUpdate() function of OpenSSL parsed very large amounts of input data. A remote attacker could use this flaw to crash an application using OpenSSL or, possibly, execute arbitrary code with the permissions of the user running that application.

CVE-2016-2109

A denial of service flaw was found in the way OpenSSL parsed certain ASN.1-encoded data from BIO (OpenSSL's I/O abstraction) inputs. An application using OpenSSL that accepted untrusted ASN.1 BIO input could be forced to allocate an excessive amount of data.

CVE-2016-0797

An integer-overflow flaw, leading to a NULL-pointer dereference or heap-based memory corruption, was found in the implementation of some BIGNUM functions of OpenSSL. Applications that use these functions with large untrusted input could crash or, potentially, execute arbitrary code.

CVE-2016-0702

A side-channel attack was found that made use of cache-bank conflicts on the Intel Sandy-Bridge microarchitecture. An attacker who had the ability to control code in a thread running on the same hyper-threaded core as the victim's thread that is performing decryption, could use this flaw to recover RSA private keys.

CVE-2016-0705

A double-free flaw was found in the way OpenSSL parsed certain malformed DSA (Digital Signature Algorithm) private keys. An attacker could create specially crafted DSA private keys that, when processed by an application compiled against OpenSSL, could cause the application to crash.

CVE-2015-3185

It was discovered that in httpd 2.4, the internal API function ap_some_auth_required() could incorrectly indicate that a request was authenticated even when no authentication had been used. An httpd module using this API function could consequently allow access that should have been denied.

CVE-2015-3195

A memory-leak vulnerability was found in the way OpenSSL parsed PKCS#7 and CMS data. A remote attacker could use this flaw to cause an application that parses PKCS#7 or CMS data from untrusted sources to use an excessive amount of memory and possibly crash.

CVE-2015-0209

A use-after-free flaw was found in the way OpenSSL imported malformed Elliptic Curve private keys. A specially crafted key file could cause an application using OpenSSL to crash when imported.

CVE-2015-3216

A regression flaw was found in the ssleay_rand_bytes() function in OpenSSL which could cause a multi-threaded application to crash.

CVE-2015-3194

A NULL-pointer dereference flaw was found in the way OpenSSL verified signatures using the RSA PSS algorithm. A remote attacker could possibly use this flaw to crash a TLS/SSL client using OpenSSL, or a TLS/SSL server using OpenSSL if it enabled client authentication.

CHAPTER 4. VERIFIED AND RESOLVED ISSUES

4.1. VERIFIED JIRAS

The following JIRAs have been verified in this release:

JBCS-72 - Solaris 11: Apache HTTP Server SSLProxyEngine: [proxy_http:error] End of file found

When using Apache Httpd on Solaris 11 as a reverse proxy with `SSLProxyEngine` enabled, a `[proxy_http:error] End of file found:` error is thrown.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-65 - LD_LIBRARY_PATH entries exported in unix session are overriden in apachectl script

The `LD_LIBRARY_PATH` variable was overridden by the `apachectl` script.

This issue is resolved in JBoss Core Services {JBCSRevision}, and `LD_LIBRARY_PATH` will no longer be modified when using `apachectl`.

JBCS-64 - StickySessions don’t work in mod_cluster for ProxyPass from unenabled context

Sticky sessions are not preserved when using `ProxyPass` from an unenabled context to an unenabled one.
This issue is resolved in JBoss Core Services {JBCSRevision}, and sticky sessions are now preserved correctly.

JBCS-62 - Ssl handshake error with LDAP secure

When using LDAP secure a `SSLException: Received fatal alert: insufficient_security` error was thrown.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-55 - ProxyErrorOverride=On causes workers in error state after 500 errors

When using `ProxyErrorOverride` to host custom error pages on Apache Httpd the worker will be marked as down if the backend replies with a 50x error code.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-54 - Unable to access deployed application via mod_cluster when balancer name contains capital letters

Previously mod_cluster was unable route requests to backends defined with capital letters, even if contexts were enabled.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-53 - mod_jk shmem segfault

There was an issue in mod_jk where `jk_shmem.hdr` would become corrupted, resulting in segfaults.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-41 - JBCS postinstall pointing to /opt/jws3-0 Solaris

The `postinstall` script on Solaris references an incorrect path.

This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-38 - apr*, libapr* modules in rhel7 zips

The **`apr*`** and **`libapr*`** modules were previously symlinks, referencing the local modules in RHEL 7 distributions.
This issue is resolved in JBoss Core Services {JBCSRevision}, as these modules are now included.

JBCS-32 - Apache Benchmark is failing on PPC64

When using **`ab`** on powerPC all requests would timeout, and the return code of **`ab`** would be 119 instead of the expected 0.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-31 - RPM: dependency on base-os 'apr-util-ldap' package from '-optional' channel

When installing JBCS on RHEL 7 there was a dependency on the **`optional`** channel for the **`apr-util-ldap`** package.
This issue is resolved in JBoss Core Services {JBCSRevision}, as a **`mod_ldap`** package has been created, and JBoss Core Services utilizes the included **`apr`** files.

JBCS-30 - ZIP: mod_security so filename contains jws3 on Windows and Solaris

The **`mod_security`** filename for Windows and Solaris systems was incorrectly **`mod_security2-jws3.so`**.
This issue is resolved in JBoss Core Services {JBCSRevision}, and is now correctly labeled **`mod_security2.so`**.

JBCS-25 - RHEL: apxs script contains variable EWS_HOME

The **`jbcs-httpd24-2.4/httpd/sbin/apxs`** script references **`EWS_HOME`**. This environment variable is used by the EWS product, and may refer to a different directory than the JBCS Apache Httpd installation.
This issue is resolved in JBoss Core Services {JBCSRevision}.

JBCS-138 - Solaris: apachectl and httpd won't start, wrong configuration directory

After installing Apache Httpd on Solaris and running the **`postinstall`** script, the service will not start due to the hardcoded path not being corrected.
This issue is resolved in JBoss Core Services {JBCSRevision}, as the **`postinstall`** script updates the path correctly.

JBCS-169 - Distribute an selinux policy in RHEL zips for httpd

The selinux RPM policy was changed; however, the zip distribution used the previous selinux policies.
This issue is resolved in JBoss Core Services {JBCSRevision}, as the zip distribution includes the latest selinux policy.

JBCS-156 - It appears that the ModSecurity module sometimes fails to increment an integer in persistent storage when many concurrent transactions are sent to the Apache web server

The ModSecurity module would sometimes fail to increment an integer in the persistent storage in case of concurrent transactions.
This issue is resolved in JBoss Core Services {JBCSRevision}.

4.2. RESOLVED ISSUES

The following issues have been included in this release, but have yet to be functionally tested:

JBCS-29 - RPM: JBCS mod_security debuginfo package conflicts with JWS one

When installing JBCS Apache Httpd on a RHEL 6 system that already contains JWS 3 packages the installation would fail, as it attempts to install mod_security from both sources.
This issue is resolved in JBoss Core Services {JBCSRevision}, as each set of packages contains the associated product name.

CHAPTER 5. KNOWN ISSUES

5.1. KNOWN ISSUES

The following is a list of known issues in this release:

JBCS-66 - Socked bind failed on link-local [IPV6]

When attempting to bind on link-local with an IPv6 address the following error is seen:

```
(22)Invalid argument: AH00072: make_sock: could not bind to address
[ffff::ffff:fff:ffff:ffff]:80
no listening sockets available, shutting down
AH00015: Unable to open logs
```

This is a known issue in JBoss Core Services {JBCSRevision}, and a workaround exists to bind the address in the configuration filewithout using the brackets. For instance, the following configuration snippet would bind correctly:

```
Listen ffff::ffff:ffff:ffff:ffff%3:80
```

JBCS-61 - Compile mod_security with JSON (libyajl) support

There is no JSON support for **`mod_security`**, and any requests made with a Content-Type of **`application/json`** that includes JSON data fails.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists.

JBCS-39 - Some extra files in zips (cache/*, config.nice, httpd.exp)

When installing JBCS via the zip distribution, additional files are found in the installation directory.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists to prevent these files from being included.

JBCS-37 - RPM: LC_MESSAGES directories installed by 'jbcs-httpd24-runtime'

On RHEL 6 x86_64 and i386 the RPM package **`jbcs-httpd24-runtime`** installs several empty directories. The RHEL 7 version of this package does not install these directories.
This is a known issue in JBoss Core Services {JBCSRevision}.

JBCS-241 - SSLOCSPEnable setting is not inherited from server config into vhost config

When **`SSLOCSPEnable`** is defined outside of **`VirtualHost`** blocks the configuration is not inherited.
This is a known issue in JBoss Core Services {JBCSRevision}, and to workaround the issue place the **`SSLOCSPEnable`** directive inside the **`VirtualHost`** configuration block.

JBCS-195 - Wrong default paths to openssl.cnf on Solaris and RHEL

The default path to the OpenSSL configuration files is incorrect. Any attempts to execute **`openssl`** on RHEL or Solaris results in the following error being thrown:

```
WARNING: can't open config file: /opt/rh/jbcs-
httpd24/root/etc/pki/tls/openssl.cnf
```

This is a known issue in JBoss Core Services {JBCSRevision}. To workaround this issue manually define the **OPENSSL_CONF** environment variable to point to the configuration file location.

JBCS-57 - CheckCaseOnly On does not stop Multiple Choices based on common basename

When **CheckCaseOnly On** is enabled and a file is requested that is not present, even with a different case, a HTTP 404 error should be thrown. Instead, a HTTP 300 error is thrown, and files with a common base name are displayed.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists at this time.

JBCS-175 - Mod_rt: log format differs from older version of mod_rt module

The log format for **mod_rt** does not correspond with the **LogFormat** defined in the httpd configuration.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists at this time.

JBCS-251 - Selinux problem during removing packages from RHEL7

When **jbcs-httpd24-mod_cluster-native** or **jbcs-httpd24-mod_bmx** are uninstalled there will be SELinux info messages included in the removal messages. For instance:

```
libsemanage.semanage_direct_remove_key: Removing last mod_cluster module
(no other mod_cluster module exists at another priority).
libsemanage.semanage_direct_remove_key: Removing last mod_bmx module (no
other mod_bmx module exists at another priority).
```

This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists at this time; however, these messages may be safely ignored.

JBCS-252 - httpd fails to start if apr/apr-util is installed prior to installing jbcs-httpd24-httpd

When installing **jbcs-httpd24-httpd** on a system that already has **apr** or **apr-util** installed **httpd** will be unable to start, and instead throw the following error:

```
Starting httpd: /opt/rh/jbcs-httpd24/root/usr/sbin/httpd: symbol lookup
error: /opt/rh/jbcs-httpd24/root/usr/sbin/httpd: undefined symbol:
apr_crypto_init
                                                           [FAILED]
```

This is a known issue in JBoss Core Services {JBCSRevision}. To workaround this issue install **jbcs-httpd24-httpd-devel**, as it contains the necessary linked libraries.

JBCS-239 - When using the zip distribution with a non-default SSLCryptoDevice on httpd (mod_ssl) httpd cannot start

The **OPENSSL_ENGINES** environment variable is not updated for the zip distrubtions, resulting in httpd failing to start when a non-default **SSLCryptoDevice** is specified. The following error is seen in Apache httpd's error log:

```
SSLCryptoDevice: Invalid argument; must be one of: 'builtin' (none),
'rdrand' (Intel RDRAND engine), 'dynamic' (Dynamic engine loading
support)
```

This is a known issue in JBoss Core Services {JBCSRevision}. To workaround this issue set **`OPENSSL_ENGINES`** to the included engines directory manually:

```
OPENSSL_ENGINES=$JBCS_HOME/httpd/lib/engines
```

JBCS-255 - Backport DeflateAlterETag directive to httpd 2.4

The **`DeflateAlterETag`** directive is not present by default, resulting in **`304 Not Modified`** responses when using **`mod_deflate`**.
This is a known issue in JBoss Core Services {JBCSRevision}. To workaround this issue the ETag header must be removed. This header may be removed by including the **`Header unset ETag`** line in the relevant configuration.

JBCS-256 - old version of openssl after groupinstall

When installing **`jbcs-httpd24`** after **`jboss-eap6`** the **`jbcs-httpd24-openssl`** package is not updated, resulting in an inability to start httpd.
This is a known issue in JBoss Core Services {JBCSRevision}. To workaround this issue manually update the package by using the following command:

```
yum update jbcs-httpd24-openssl
```

JBCS-257 - graceful start failure due to wrong path to /sbin/apachectl

When attempting to execute **`service jbcs-httpd24-httpd configtest`** or **`service jbcs-httpd24-httpd graceful`** the following error is thrown:

```
/usr/libexec/initscripts/legacy-actions/jbcs-httpd24-httpd/graceful:
line 2: /sbin/apachectl: No such file or directory
```

This is a known issue in JBoss Core Services {JBCSRevision}. To workaround this issue perform the following steps:

1. Include the correct path in **`/usr/libexec/initscripts/legacy-actions/jbcs-httpd24-httpd/configtest`**, as seen below:

   ```
   #!/bin/sh
   exec /opt/rh/jbcs-httpd24/root/usr/sbin/apachectl configtest "$@"
   ```

2. Include the correct path in **`/usr/libexec/initscripts/legacy-actions/jbcs-httpd24-httpd/graceful`**, as seen below:

   ```
   #!/bin/sh
   exec /opt/rh/jbcs-httpd24/root/usr/sbin/apachectl graceful "$@"
   ```

JBCS-258 - Directive SSLOCSPResponderCertificateFile is missing from EWS 3.0.x

The **`SSLOCSPResponderCertificateFile`** is not included in the distribution.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists at this time.

JBCS-309 - JON Httpd: start failed after configuration new Listen port in JON

Using JON with JBoss Web Server, if you add a new **`Listen`** port to an Apache HTTP Server may result in the Apache HTTP Server not able to restart. This is because the **`Listen`** directive is added at the end of **`httpd.conf`** even though it may already be defined in **`conf.d/ssl.conf`**. This issue will be fixed in a future release.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists at this time.

JBCS-298 - ProxyPass worker name (http://localhost:3128/...) too long

By default, the maximum length of ProxyPass worker name is 96. If the worker name exceeds this limit, an error is displayed.
This is a known issue in JBoss Core Services {JBCSRevision}, and no workaround exists at this time.

JBCS-265 - apxs binary missing from Sun and Windows builds

The apxs binary is missing in the Sun and Windows builds.
This is a known issue in JBoss Core Services {JBCSRevision}, and the devel packages and debug symbols are provided on-demand.