[RHSA-2022:7143-01] Important: Red Hat JBoss Core Servi...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=21690

Author
SecurityHome.eu

Published: 27 October 2022

==========
Red Hat Security Advisory

Synopsis: Important: Red Hat JBoss Core Services Apache HTTP Server 2.4.51 security update
Advisory ID: RHSA-2022:7143-01
Product: Red Hat JBoss Core Services
Advisory URL: https://access.redhat.com/errata/RHSA-2022:7143
Issue date: 2022-10-26
CVE Names: CVE-2021-33193 CVE-2021-36160 CVE-2021-39275
CVE-2021-41524 CVE-2021-44224 CVE-2021-45960
CVE-2021-46143 CVE-2022-22822 CVE-2022-22823
CVE-2022-22824 CVE-2022-22825 CVE-2022-22826
CVE-2022-22827 CVE-2022-23852 CVE-2022-23990
CVE-2022-25235 CVE-2022-25236 CVE-2022-25313
CVE-2022-25314 CVE-2022-25315
==========
1. Summary:

An update is now available for Red Hat JBoss Core Services.

Red Hat Product Security has rated this update as having a security impact
of Important. A Common Vulnerability Scoring System (CVSS) base score,
which gives a detailed severity rating, is available for each vulnerability
from the CVE link(s) in the References section.

2. Relevant releases/architectures:

Red Hat JBoss Core Services on RHEL 7 Server - noarch, x86_64
Red Hat JBoss Core Services on RHEL 8 - noarch, x86_64

3. Description:

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.

This release of Red Hat JBoss Core Services Apache HTTP Server 2.4.51 serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 10, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Security Fix(es):

* expat: Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution (CVE-2022-25235)

* expat: Namespace-separator characters in "xmlns[:prefix]" attribute values can lead to arbitrary code execution (CVE-2022-25236)

* expat: Integer overflow in storeRawNames() (CVE-2022-25315)

* httpd: Request splitting via HTTP/2 method injection and mod_proxy (CVE-2021-33193)

* httpd: mod_proxy_uwsgi: out-of-bounds read via a crafted request uri-path (CVE-2021-36160)

* httpd: Out-of-bounds write in ap_escape_quotes() via malicious input (CVE-2021-39275)

* httpd: NULL pointer dereference via crafted request during HTTP/2 request processing (CVE-2021-41524)

* httpd: possible NULL dereference or SSRF in forward proxy configurations (CVE-2021-44224)

* expat: Large number of prefixed XML attributes on a single tag can crash libexpat (CVE-2021-45960)

* expat: Integer overflow in doProlog in xmlparse.c (CVE-2021-46143)

* expat: Integer overflow in addBinding in xmlparse.c (CVE-2022-22822)

* expat: Integer overflow in build_model in xmlparse.c (CVE-2022-22823)

* expat: Integer overflow in defineAttribute in xmlparse.c (CVE-2022-22824)

* expat: Integer overflow in lookup in xmlparse.c (CVE-2022-22825)

* expat: Integer overflow in nextScaffoldPart in xmlparse.c
(CVE-2022-22826)

* expat: Integer overflow in storeAtts in xmlparse.c (CVE-2022-22827)

* expat: Integer overflow in function XML_GetBuffer (CVE-2022-23852)

* expat: stack exhaustion in doctype parsing (CVE-2022-25313)

* expat: integer overflow in copyString() (CVE-2022-25314)

* expat: integer overflow in the doProlog function (CVE-2022-23990)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

4. Solution:

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

Applications using the APR libraries, such as httpd, must be restarted for this update to take effect. After installing the updated packages, the httpd daemon will be restarted automatically.

5. Bugs fixed (https://bugzilla.redhat.com/):

1966728 - CVE-2021-33193 httpd: Request splitting via HTTP/2 method injection and mod_proxy
2005119 - CVE-2021-39275 httpd: Out-of-bounds write in ap_escape_quotes() via malicious input
2005124 - CVE-2021-36160 httpd: mod_proxy_uwsgi: out-of-bounds read via a crafted request uri-path
2010934 - CVE-2021-41524 httpd: NULL pointer dereference via crafted request during HTTP/2 request processing
2034672 - CVE-2021-44224 httpd: possible NULL dereference or SSRF in forward proxy configurations
2044451 - CVE-2021-45960 expat: Large number of prefixed XML attributes on a single tag can crash libexpat
2044455 - CVE-2021-46143 expat: Integer overflow in doProlog in xmlparse.c
2044457 - CVE-2022-22822 expat: Integer overflow in addBinding in xmlparse.c
2044464 - CVE-2022-22823 expat: Integer overflow in build_model in xmlparse.c
2044467 - CVE-2022-22824 expat: Integer overflow in defineAttribute in xmlparse.c
2044479 - CVE-2022-22825 expat: Integer overflow in lookup in xmlparse.c
2044484 - CVE-2022-22826 expat: Integer overflow in nextScaffoldPart in xmlparse.c
2044488 - CVE-2022-22827 expat: Integer overflow in storeAtts in xmlparse.c
2044613 - CVE-2022-23852 expat: Integer overflow in function XML_GetBuffer
2048356 - CVE-2022-23990 expat: integer overflow in the doProlog function
2056350 - CVE-2022-25313 expat: stack exhaustion in doctype parsing

2056354 - CVE-2022-25314 expat: integer overflow in copyString()
2056363 - CVE-2022-25315 expat: Integer overflow in storeRawNames()
2056366 - CVE-2022-25235 expat: Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution
2056370 - CVE-2022-25236 expat: Namespace-separator characters in "xmlns[:prefix]" attribute values can lead to arbitrary code execution

6. Package List:

Red Hat JBoss Core Services on RHEL 7 Server:

Source:
jbcs-httpd24-apr-1.7.0-6.el7jbcs.src.rpm
jbcs-httpd24-apr-util-1.6.1-98.el7jbcs.src.rpm
jbcs-httpd24-brotli-1.0.9-2.el7jbcs.src.rpm
jbcs-httpd24-curl-7.83.1-6.el7jbcs.src.rpm
jbcs-httpd24-httpd-2.4.51-28.el7jbcs.src.rpm
jbcs-httpd24-jansson-2.14-1.el7jbcs.src.rpm
jbcs-httpd24-mod_http2-1.15.19-17.el7jbcs.src.rpm
jbcs-httpd24-mod_jk-1.2.48-41.redhat_1.el7jbcs.src.rpm
jbcs-httpd24-mod_md-2.4.0-15.el7jbcs.src.rpm
jbcs-httpd24-mod_proxy_cluster-1.3.17-9.el7jbcs.src.rpm
jbcs-httpd24-mod_security-2.9.3-19.el7jbcs.src.rpm
jbcs-httpd24-nghttp2-1.43.0-10.el7jbcs.src.rpm
jbcs-httpd24-openssl-1.1.1k-12.el7jbcs.src.rpm
jbcs-httpd24-openssl-chil-1.0.0-16.el7jbcs.src.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-31.el7jbcs.src.rpm

noarch:
jbcs-httpd24-httpd-manual-2.4.51-28.el7jbcs.noarch.rpm

x86_64:
jbcs-httpd24-apr-1.7.0-6.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-debuginfo-1.7.0-6.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-devel-1.7.0-6.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-debuginfo-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-devel-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-ldap-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-mysql-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-nss-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-odbc-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-openssl-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-pgsql-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-apr-util-sqlite-1.6.1-98.el7jbcs.x86_64.rpm
jbcs-httpd24-brotli-1.0.9-2.el7jbcs.x86_64.rpm
jbcs-httpd24-brotli-debuginfo-1.0.9-2.el7jbcs.x86_64.rpm
jbcs-httpd24-brotli-devel-1.0.9-2.el7jbcs.x86_64.rpm

jbcs-httpd24-curl-7.83.1-6.el7jbcs.x86_64.rpm
jbcs-httpd24-curl-debuginfo-7.83.1-6.el7jbcs.x86_64.rpm
jbcs-httpd24-httpd-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-httpd-debuginfo-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-httpd-devel-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-httpd-selinux-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-httpd-tools-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-jansson-2.14-1.el7jbcs.x86_64.rpm
jbcs-httpd24-jansson-debuginfo-2.14-1.el7jbcs.x86_64.rpm
jbcs-httpd24-jansson-devel-2.14-1.el7jbcs.x86_64.rpm
jbcs-httpd24-libcurl-7.83.1-6.el7jbcs.x86_64.rpm
jbcs-httpd24-libcurl-devel-7.83.1-6.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_http2-1.15.19-17.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_http2-debuginfo-1.15.19-17.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_jk-ap24-1.2.48-41.redhat_1.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_jk-debuginfo-1.2.48-41.redhat_1.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_ldap-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_md-2.4.0-15.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_md-debuginfo-2.4.0-15.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_cluster-1.3.17-9.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_cluster-debuginfo-1.3.17-9.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_html-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_security-2.9.3-19.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_security-debuginfo-2.9.3-19.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_session-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-mod_ssl-2.4.51-28.el7jbcs.x86_64.rpm
jbcs-httpd24-nghttp2-1.43.0-10.el7jbcs.x86_64.rpm
jbcs-httpd24-nghttp2-debuginfo-1.43.0-10.el7jbcs.x86_64.rpm
jbcs-httpd24-nghttp2-devel-1.43.0-10.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-1.1.1k-12.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-chil-1.0.0-16.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-chil-debuginfo-1.0.0-16.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-debuginfo-1.1.1k-12.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-devel-1.1.1k-12.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-libs-1.1.1k-12.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-perl-1.1.1k-12.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-31.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-pkcs11-debuginfo-0.4.10-31.el7jbcs.x86_64.rpm
jbcs-httpd24-openssl-static-1.1.1k-12.el7jbcs.x86_64.rpm

Red Hat JBoss Core Services on RHEL 8:

Source:
jbcs-httpd24-apr-1.7.0-6.el8jbcs.src.rpm
jbcs-httpd24-apr-util-1.6.1-98.el8jbcs.src.rpm
jbcs-httpd24-brotli-1.0.9-2.el8jbcs.src.rpm
jbcs-httpd24-curl-7.83.1-6.el8jbcs.src.rpm
jbcs-httpd24-httpd-2.4.51-28.el8jbcs.src.rpm

jbcs-httpd24-jansson-2.14-1.el8jbcs.src.rpm
jbcs-httpd24-mod_http2-1.15.19-17.el8jbcs.src.rpm
jbcs-httpd24-mod_jk-1.2.48-41.redhat_1.el8jbcs.src.rpm
jbcs-httpd24-mod_md-2.4.0-15.el8jbcs.src.rpm
jbcs-httpd24-mod_proxy_cluster-1.3.17-9.el8jbcs.src.rpm
jbcs-httpd24-mod_security-2.9.3-19.el8jbcs.src.rpm
jbcs-httpd24-nghttp2-1.43.0-10.el8jbcs.src.rpm
jbcs-httpd24-openssl-1.1.1k-12.el8jbcs.src.rpm
jbcs-httpd24-openssl-chil-1.0.0-16.el8jbcs.src.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-31.el8jbcs.src.rpm

noarch:
jbcs-httpd24-httpd-manual-2.4.51-28.el8jbcs.noarch.rpm

x86_64:
jbcs-httpd24-apr-1.7.0-6.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-debuginfo-1.7.0-6.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-devel-1.7.0-6.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-devel-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-ldap-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-ldap-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-mysql-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-mysql-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-nss-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-nss-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-odbc-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-odbc-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-openssl-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-openssl-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-pgsql-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-pgsql-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-sqlite-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-apr-util-sqlite-debuginfo-1.6.1-98.el8jbcs.x86_64.rpm
jbcs-httpd24-brotli-1.0.9-2.el8jbcs.x86_64.rpm
jbcs-httpd24-brotli-debuginfo-1.0.9-2.el8jbcs.x86_64.rpm
jbcs-httpd24-brotli-devel-1.0.9-2.el8jbcs.x86_64.rpm
jbcs-httpd24-curl-7.83.1-6.el8jbcs.x86_64.rpm
jbcs-httpd24-curl-debuginfo-7.83.1-6.el8jbcs.x86_64.rpm
jbcs-httpd24-httpd-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-httpd-debuginfo-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-httpd-devel-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-httpd-selinux-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-httpd-tools-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-httpd-tools-debuginfo-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-jansson-2.14-1.el8jbcs.x86_64.rpm
jbcs-httpd24-jansson-debuginfo-2.14-1.el8jbcs.x86_64.rpm

jbcs-httpd24-jansson-devel-2.14-1.el8jbcs.x86_64.rpm
jbcs-httpd24-libcurl-7.83.1-6.el8jbcs.x86_64.rpm
jbcs-httpd24-libcurl-debuginfo-7.83.1-6.el8jbcs.x86_64.rpm
jbcs-httpd24-libcurl-devel-7.83.1-6.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_http2-1.15.19-17.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_http2-debuginfo-1.15.19-17.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_jk-ap24-1.2.48-41.redhat_1.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_jk-ap24-debuginfo-1.2.48-41.redhat_1.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_ldap-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_ldap-debuginfo-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_md-2.4.0-15.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_md-debuginfo-2.4.0-15.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_cluster-1.3.17-9.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_cluster-debuginfo-1.3.17-9.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_html-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_proxy_html-debuginfo-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_security-2.9.3-19.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_security-debuginfo-2.9.3-19.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_session-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_session-debuginfo-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_ssl-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-mod_ssl-debuginfo-2.4.51-28.el8jbcs.x86_64.rpm
jbcs-httpd24-nghttp2-1.43.0-10.el8jbcs.x86_64.rpm
jbcs-httpd24-nghttp2-debuginfo-1.43.0-10.el8jbcs.x86_64.rpm
jbcs-httpd24-nghttp2-devel-1.43.0-10.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-1.1.1k-12.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-chil-1.0.0-16.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-chil-debuginfo-1.0.0-16.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-debuginfo-1.1.1k-12.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-devel-1.1.1k-12.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-libs-1.1.1k-12.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-libs-debuginfo-1.1.1k-12.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-perl-1.1.1k-12.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-31.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-pkcs11-debuginfo-0.4.10-31.el8jbcs.x86_64.rpm
jbcs-httpd24-openssl-static-1.1.1k-12.el8jbcs.x86_64.rpm

These packages are GPG signed by Red Hat for security. Our key and
details on how to verify the signature are available from
https://access.redhat.com/security/team/key/

7. References:

https://access.redhat.com/security/cve/CVE-2021-33193
https://access.redhat.com/security/cve/CVE-2021-36160
https://access.redhat.com/security/cve/CVE-2021-39275
https://access.redhat.com/security/cve/CVE-2021-41524
https://access.redhat.com/security/cve/CVE-2021-44224

https://access.redhat.com/security/cve/CVE-2021-45960
https://access.redhat.com/security/cve/CVE-2021-46143
https://access.redhat.com/security/cve/CVE-2022-22822
https://access.redhat.com/security/cve/CVE-2022-22823
https://access.redhat.com/security/cve/CVE-2022-22824
https://access.redhat.com/security/cve/CVE-2022-22825
https://access.redhat.com/security/cve/CVE-2022-22826
https://access.redhat.com/security/cve/CVE-2022-22827
https://access.redhat.com/security/cve/CVE-2022-23852
https://access.redhat.com/security/cve/CVE-2022-23990
https://access.redhat.com/security/cve/CVE-2022-25235
https://access.redhat.com/security/cve/CVE-2022-25236
https://access.redhat.com/security/cve/CVE-2022-25313
https://access.redhat.com/security/cve/CVE-2022-25314
https://access.redhat.com/security/cve/CVE-2022-25315
https://access.redhat.com/security/updates/classification/#important

8. Contact:

The Red Hat security contact is <secalert@redhat.com>. More contact
details at https://access.redhat.com/security/team/contact/