[RHSA-2021:1199-01] Important: Red Hat JBoss Core Servi...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=18708

Author
SecurityHome.eu

Published: 14 April 2021

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

Synopsis: Important: Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP7 security update
Advisory ID: RHSA-2021:1199-01
Product: Red Hat JBoss Core Services
Advisory URL: https://access.redhat.com/errata/RHSA-2021:1199
Issue date: 2021-04-14
CVE Names: CVE-2021-3449 CVE-2021-3450
==========
1. Summary:

Updated packages that provide Red Hat JBoss Core Services Pack Apache Server 2.4.37 and fix several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 7.

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, ppc64, x86_64

3. Description:

This release adds the new Apache HTTP Server 2.4.37 Service Pack 7 packages that are part of the JBoss Core Services offering.

This release serves as a replacement for Red Hat JBoss Core Services Pack Apache Server 2.4.37 Service Pack 6 and includes bug fixes and enhancements. Refer to the Release Notes for information on the most

significant bug fixes and enhancements included in this release.

Security fix(es):

* openssl: NULL pointer dereference in signature_algorithms processing (CVE-2021-3449)
* openssl: CA certificate check bypass with X509_V_FLAG_X509_STRICT (CVE-2021-3450)

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:

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

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

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

1941547 - CVE-2021-3450 openssl: CA certificate check bypass with X509_V_FLAG_X509_STRICT
1941554 - CVE-2021-3449 openssl: NULL pointer dereference in signature_algorithms processing

6. Package List:

Red Hat JBoss Core Services on RHEL 7 Server:

Source:
jbcs-httpd24-httpd-2.4.37-70.jbcs.el7.src.rpm
jbcs-httpd24-mod_cluster-native-1.3.14-20.Final_redhat_2.jbcs.el7.src.rpm
jbcs-httpd24-mod_http2-1.15.7-14.jbcs.el7.src.rpm
jbcs-httpd24-mod_jk-1.2.48-13.redhat_1.jbcs.el7.src.rpm
jbcs-httpd24-mod_md-2.0.8-33.jbcs.el7.src.rpm
jbcs-httpd24-mod_security-2.9.2-60.GA.jbcs.el7.src.rpm
jbcs-httpd24-nghttp2-1.39.2-37.jbcs.el7.src.rpm
jbcs-httpd24-openssl-1.1.1g-6.jbcs.el7.src.rpm
jbcs-httpd24-openssl-chil-1.0.0-5.jbcs.el7.src.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-20.jbcs.el7.src.rpm

noarch:
jbcs-httpd24-httpd-manual-2.4.37-70.jbcs.el7.noarch.rpm

ppc64:
jbcs-httpd24-mod_http2-1.15.7-14.jbcs.el7.ppc64.rpm

jbcs-httpd24-mod_http2-debuginfo-1.15.7-14.jbcs.el7.ppc64.rpm
jbcs-httpd24-mod_md-2.0.8-33.jbcs.el7.ppc64.rpm
jbcs-httpd24-mod_md-debuginfo-2.0.8-33.jbcs.el7.ppc64.rpm
jbcs-httpd24-openssl-chil-1.0.0-5.jbcs.el7.ppc64.rpm
jbcs-httpd24-openssl-chil-debuginfo-1.0.0-5.jbcs.el7.ppc64.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-20.jbcs.el7.ppc64.rpm
jbcs-httpd24-openssl-pkcs11-debuginfo-0.4.10-20.jbcs.el7.ppc64.rpm

x86_64:
jbcs-httpd24-httpd-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-httpd-debuginfo-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-httpd-devel-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-httpd-selinux-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-httpd-tools-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_cluster-native-1.3.14-20.Final_redhat_2.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_cluster-native-debuginfo-1.3.14-20.Final_redhat_2.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_http2-1.15.7-14.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_http2-debuginfo-1.15.7-14.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_jk-ap24-1.2.48-13.redhat_1.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_jk-debuginfo-1.2.48-13.redhat_1.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_jk-manual-1.2.48-13.redhat_1.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_ldap-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_md-2.0.8-33.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_md-debuginfo-2.0.8-33.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_proxy_html-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_security-2.9.2-60.GA.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_security-debuginfo-2.9.2-60.GA.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_session-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-mod_ssl-2.4.37-70.jbcs.el7.x86_64.rpm
jbcs-httpd24-nghttp2-1.39.2-37.jbcs.el7.x86_64.rpm
jbcs-httpd24-nghttp2-debuginfo-1.39.2-37.jbcs.el7.x86_64.rpm
jbcs-httpd24-nghttp2-devel-1.39.2-37.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-1.1.1g-6.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-chil-1.0.0-5.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-chil-debuginfo-1.0.0-5.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-debuginfo-1.1.1g-6.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-devel-1.1.1g-6.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-libs-1.1.1g-6.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-perl-1.1.1g-6.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-pkcs11-0.4.10-20.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-pkcs11-debuginfo-0.4.10-20.jbcs.el7.x86_64.rpm
jbcs-httpd24-openssl-static-1.1.1g-6.jbcs.el7.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-2021-3449
https://access.redhat.com/security/cve/CVE-2021-3450
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/