RHSA-2018:2486 - Security Advisory

Issued: 2018-08-16 Updated: 2018-08-16

Overview

Synopsis

Important: Red Hat JBoss Core Services Apache HTTP Server 2.4.29 security update

Type/Severity

Security Advisory: Important

Topic

Red Hat JBoss Core Services Pack Apache Server 2.4.29 packages for Microsoft Windows and Oracle Solaris are now available.

Red Hat Product Security has rated this release 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.

Description

This release adds the new Apache HTTP Server 2.4.29 packages that are part of the JBoss Core Services offering.

This release serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.23, and includes bug fixes and enhancements. Refer to the Release Notes for information on the most significant bug fixes, enhancements and component upgrades included in this release.

Security Fix(es):

- expat: Out-of-bounds heap read on crafted input causing crash (CVE-2016-0718)
- curl: escape and unescape integer overflows (CVE-2016-7167)
- curl: Cookie injection for other servers (CVE-2016-8615)
- curl: Case insensitive password comparison (CVE-2016-8616)
- curl: Out-of-bounds write via unchecked multiplication (CVE-2016-8617)
- curl: Double-free in curl_maprintf (CVE-2016-8618)
- curl: Double-free in krb5 code (CVE-2016-8619)
- curl: curl_getdate out-of-bounds read (CVE-2016-8621)
- curl: URL unescape heap overflow via integer truncation (CVE-2016-8622)
- curl: Use-after-free via shared cookies (CVE-2016-8623)
- curl: Invalid URL parsing with '#' (CVE-2016-8624)
- curl: IDNA 2003 makes curl use wrong host (CVE-2016-8625)
- libxml2: out-of-bounds read (unfixed CVE-2016-4483 in JBCS) (CVE-2016-9598)
- pcre: Out-of-bounds read in compile_bracket_matchingpath function (8.41/3) (CVE-2017-6004)
- pcre: Invalid Unicode property lookup (8.41/7, 10.24/2) (CVE-2017-7186)
- pcre: invalid memory read in_pcre32_xclass (pcre_xclass.c) (CVE-2017-7244)
- pcre: stack-based buffer overflow write in pcre32_copy_substring (CVE-2017-7245)
- pcre: stack-based buffer overflow write in pcre32_copy_substring (CVE-2017-7246)
- curl: FTP PWD response parser out of bounds read (CVE-2017-1000254)
- curl: IMAP FETCH response out of bounds read (CVE-2017-1000257)
- curl: Heap-based buffer overflow in Curl_smtp_escape_eob() when uploading data over SMTP (CVE-2018-0500)

Details around this issue, including information about the CVE, severity of the issue, and the CVSS score can be found on the CVE page listed in the Reference section below.

The following packages have been upgraded to a newer upstream version:

- Curl (7.57.0)
- OpenSSL (1.0.2n)
- Expat (2.2.5)
- PCRE (8.41)
- libxml2 (2.9.7)

Acknowledgements:

CVE-2017-1000254: Red Hat would like to thank Daniel Stenberg for reporting this issue. Upstream acknowledges Max Dymond as the original reporter.
CVE-2017-1000257: Red Hat would like to thank the Curl project for reporting this issue. Upstream

acknowledges Brian Carpenter, (the OSS-Fuzz project) as the original reporter.
CVE-2018-0500: Red Hat would like to thank the Curl project for reporting this issue.

Solution

The References section of this erratum contains a download link (you must log in to download the update). Before applying the update, back up your existing Red Hat JBoss Core Services installation (including all applications and configuration files).

Affected Products

- Red Hat JBoss Core Services Text-Only Advisories x86_64

Fixes

- BZ - 1296102 - CVE-2016-0718 expat: Out-of-bounds heap read on crafted input causing crash
- BZ - 1375906 - CVE-2016-7167 curl: escape and unescape integer overflows
- BZ - 1388370 - CVE-2016-8615 curl: Cookie injection for other servers
- BZ - 1388371 - CVE-2016-8616 curl: Case insensitive password comparison
- BZ - 1388377 - CVE-2016-8617 curl: Out-of-bounds write via unchecked multiplication
- BZ - 1388378 - CVE-2016-8618 curl: Double-free in curl_maprintf
- BZ - 1388379 - CVE-2016-8619 curl: Double-free in krb5 code
- BZ - 1388385 - CVE-2016-8621 curl: curl_getdate out-of-bounds read
- BZ - 1388386 - CVE-2016-8622 curl: URL unescape heap overflow via integer truncation
- BZ - 1388388 - CVE-2016-8623 curl: Use-after-free via shared cookies
- BZ - 1388390 - CVE-2016-8624 curl: Invalid URL parsing with '#'
- BZ - 1388392 - CVE-2016-8625 curl: IDNA 2003 makes curl use wrong host
- BZ - 1408306 - CVE-2016-9598 libxml2: out-of-bounds read (unfixed CVE-2016-4483 in JBCS)
- BZ - 1425365 - CVE-2017-6004 pcre: Out-of-bounds read in compile_bracket_matchingpath function (8.41/3)
- BZ - 1434504 - CVE-2017-7186 pcre: Invalid Unicode property lookup (8.41/7, 10.24/2)
- BZ - 1437364 - CVE-2017-7244 pcre: invalid memory read in _pcre32_xclass (pcre_xclass.c)
- BZ - 1437367 - CVE-2017-7245 pcre: stack-based buffer overflow write in pcre32_copy_substring
- BZ - 1437369 - CVE-2017-7246 pcre: stack-based buffer overflow write in pcre32_copy_substring
- BZ - 1495541 - CVE-2017-1000254 curl: FTP PWD response parser out of bounds read
- BZ - 1503705 - CVE-2017-1000257 curl: IMAP FETCH response out of bounds read
- BZ - 1597101 - CVE-2018-0500 curl: Heap-based buffer overflow in Curl_smtp_escape_eob() when uploading data over SMTP

CVEs

- CVE-2016-0718
- CVE-2016-4975
- CVE-2016-5131
- CVE-2016-7167
- CVE-2016-8615
- CVE-2016-8616
- CVE-2016-8617
- CVE-2016-8618
- CVE-2016-8619
- CVE-2016-8621
- CVE-2016-8622
- CVE-2016-8623
- CVE-2016-8624
- CVE-2016-8625
- CVE-2016-9318
- CVE-2016-9596
- CVE-2016-9597
- CVE-2016-9598
- CVE-2017-6004
- CVE-2017-7186
- CVE-2017-7244
- CVE-2017-7245
- CVE-2017-7246
- CVE-2017-9047
- CVE-2017-9048
- CVE-2017-9049
- CVE-2017-9050
- CVE-2017-18258
- CVE-2017-1000254
- CVE-2017-1000257
- CVE-2018-0500

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/documentation/en-us/red_hat_jboss_core_services/2.4.29/html-single/red_hat_jboss_core_services_apache_http_server_2.4.29_release_notes/

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