RHSA-2025:13681 - Security Advisory

Issued: 2025-08-14 Updated: 2025-08-14

Overview

Synopsis

Important: Red Hat JBoss Core Services Apache HTTP Server 2.4.62 SP1 security update

Type/Severity

Security Advisory: Important

Topic

Red Hat JBoss Core Services Apache HTTP Server 2.4.62 Service Pack 1 is now available.

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.

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 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 2.4.62 Service Pack 1 serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.62, and includes bug fixes and enhancements, which are documented in the Release Notes linked to in the References section.

Security Fix(es):

- expat: Improper Restriction of XML Entity Expansion Depth in libexpat [jbcs-httpd-2.4] (CVE-2024-8176)
- httpd: HTTP Session Hijack via a TLS upgrade [jbcs-httpd-2.4] (CVE-2025-49812)
- httpd: access control bypass by trusted clients is possible using TLS 1.3 session resumption [jbcs-httpd-2.4] (CVE-2025-23048)
- httpd: insufficient escaping of user-supplied data in mod_ssl [jbcs-httpd-2.4] (CVE-2024-47252)
- httpd: untrusted input from a client causes an assertion to fail in the Apache mod_proxy_http2 module [jbcs-httpd-2.4] (CVE-2025-49630)
- libxml2: Out-of-Bounds Read in libxml2 [jbcs-httpd-2.4] (CVE-2025-32414)
- libxml2: Out-of-bounds Read in xmlSchemaIDCFillNodeTables [jbcs-httpd-2.4] (CVE-2025-32415)
- jbcs-httpd24-mod_security: ModSecurity Has Possible DoS Vulnerability [jbcs-httpd-2.4] (CVE-2025-47947)

A Red Hat Security Bulletin which addresses further details about this flaw is available in the References section.

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.

Solution

Before applying the update, back up your existing installation, including all applications, configuration files, databases and database settings, and so on.

The References section of this erratum contains a download link. You must be logged in to download the update.

Affected Products

- Red Hat JBoss Core Services Text-Only Advisories x86_64

Fixes

- BZ - 2310137 - CVE-2024-8176 libexpat: expat: Improper Restriction of XML Entity Expansion Depth in libexpat

- BZ - 2358121 - CVE-2025-32414 libxml2: Out-of-Bounds Read in libxml2
- BZ - 2360768 - CVE-2025-32415 libxml2: Out-of-bounds Read in xmlSchemaIDCFillNodeTables
- BZ - 2367903 - CVE-2025-47947 modsecurity: ModSecurity Has Possible DoS Vulnerability
- BZ - 2374571 - CVE-2024-47252 httpd: insufficient escaping of user-supplied data in mod_ssl
- BZ - 2374576 - CVE-2025-23048 httpd: mod_ssl: access control bypass by trusted clients is possible using TLS 1.3 session resumption
- BZ - 2374578 - CVE-2025-49630 httpd: mod_proxy_http2: untrusted input from a client causes an assertion to fail in the Apache mod_proxy_http2 module
- BZ - 2374580 - CVE-2025-49812 httpd: HTTP Session Hijack via a TLS upgrade

CVEs

- CVE-2024-8176
- CVE-2024-47252
- CVE-2025-23048
- CVE-2025-32414
- CVE-2025-32415
- CVE-2025-47947
- CVE-2025-49630
- CVE-2025-49812

References

- https://access.redhat.com/security/updates/classification/#important
- https://docs.redhat.com/en/documentation/red_hat_jboss_core_services/2.4.62/html/red_hat_jboss_core_services_apache_http_server_2.4.62_serv

---

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

Red Hat Summit