RHSA-2025:19020 - Security Advisory

Issued: 2025-10-27 Updated: 2025-10-27

Overview

Synopsis

Important: Red Hat JBoss Core Services Apache HTTP Server 2.4.62 SP2 security update

Type/Severity

Security Advisory: Important

Topic

Red Hat JBoss Core Services Apache HTTP Server 2.4.62 Service Pack 2 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 2 serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.62 Service Pack 1, and includes bug fixes and enhancements, which are documented in the Release Notes linked to in the References section.

Security Fix(es):

- expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing [jbcs-httpd-2.4] (CVE-2025-59375)
- libxml2: Heap use after free (UAF) leads to Denial of service (DoS) [jbcs-httpd-2.4] (CVE-2025-49794)
- libxml2: Null pointer dereference leads to Denial of service (DoS) [jbcs-httpd-2.4] (CVE-2025-49795)
- libxml2: Type confusion leads to Denial of service (DoS) [jbcs-httpd-2.4] (CVE-2025-49796)
- libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2 [jbcs-httpd-2.4] (CVE-2025-6021)

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 - 2372373 - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- BZ - 2372379 - CVE-2025-49795 libxml: Null pointer dereference leads to Denial of service (DoS)

- BZ - 2372385 - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- BZ - 2372406 - CVE-2025-6021 libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2
- BZ - 2395108 - CVE-2025-59375 expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing

CVEs

- CVE-2025-6021
- CVE-2025-49794
- CVE-2025-49795
- CVE-2025-49796
- CVE-2025-59375

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/.