



Red Hat Product Errata

RHSA-2025

Overview

Synopsis

Important: Red Hat

Type/Severity

Security Advisory:

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)

About cookies on this site

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for cross-context behavioral advertising. This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act of 2018 ("CCPA") as amended by the California Privacy Rights Act of 2020 ("CPRA"). You can make choices using the buttons below to allow or prevent such uses.

dated: 2025-10-27

- [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

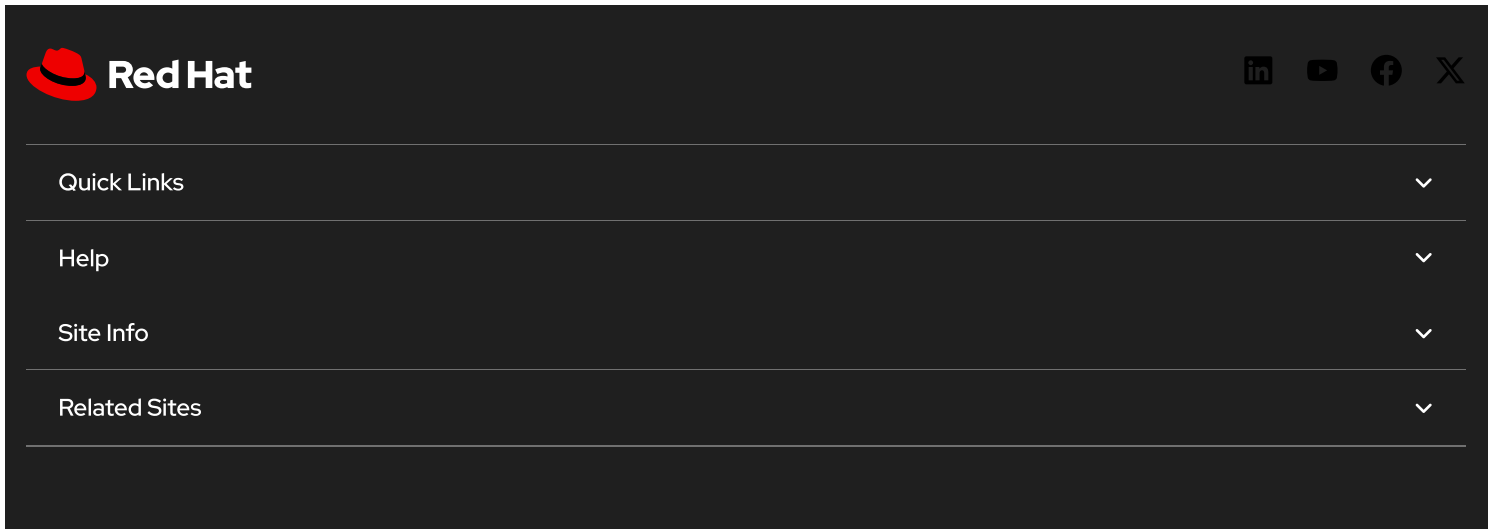
CVEs

- [CVE-2025-6021](#)
- [CVE-2025-49794](#)
- [CVE-2025-49795](#)
- [CVE-2025-49796](#)
- [CVE-2025-59375](#)

References

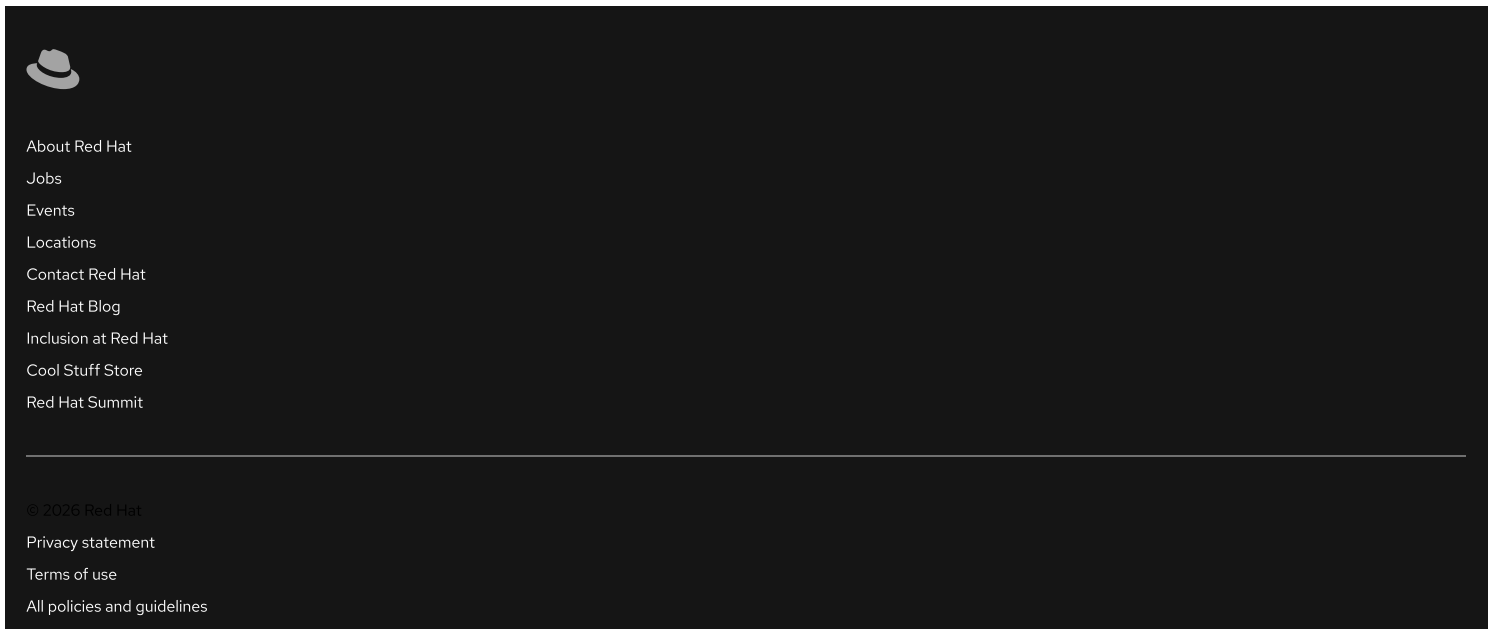
- <https://access.redhat.com/security/updates/classification/#important>
- https://docs.redhat.com/en/documentation/red_hat_jboss_core_services/2.4.62/html/red_hat_jboss_core_services_apache_http_server_2.4.62_serv

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



The image shows the Red Hat logo and a navigation menu with the following items: Quick Links, Help, Site Info, and Related Sites. Each item has a downward arrow indicating a dropdown menu. In the top right corner, there are social media icons for LinkedIn, YouTube, Facebook, and X.

✓ All systems operational



The image shows a footer navigation menu with the following items: About Red Hat, Jobs, Events, Locations, Contact Red Hat, Red Hat Blog, Inclusion at Red Hat, Cool Stuff Store, and Red Hat Summit. At the bottom, there are links for © 2026 Red Hat, Privacy statement, Terms of use, and All policies and guidelines.

Digital accessibility

Cookie Preferences and Do Not Sell or Share My Personal Information