



Red Hat Product Errata    RHSA-2025:22033 - Security Advisory

# RHSA-2025:22033 - Security Advisory

Issued: 2025-11-25    Updated: 2025-11-25

[Overview](#)[Updated Packages](#)

## Synopsis

Important: expat security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#)

## Topic

An update for expat is now available for Red Hat Enterprise Linux 9.4 Extended Update Support.

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

Expat is a C library for parsing XML documents.

Security Fix(es):

- libexpat: expat: Improper Restriction of XML Entity Expansion Depth in libexpat (CVE-2024-8176)
- expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing (CVE-2025-59375)

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



For details on how to apply this update, which includes the changes described in this advisory, refer to:

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

## Affected Products

- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 9.4 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.4 x86\_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 9.4 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x

## Fixes

- [BZ - 2310137](#)  - CVE-2024-8176 libexpat: expat: Improper Restriction of XML Entity Expansion Depth in libexpat
- [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-2024-8176](#)
- [CVE-2025-59375](#)

## References

- <https://access.redhat.com/security/updates/classification/#important>

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



The image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items: "Quick Links", "Help", "Site Info", and "Related Sites", each with a downward-pointing chevron icon to its right.

✓ All systems operational



The image shows a dark-themed footer navigation menu. It starts with a small icon of a hat. Below the icon are three links: "About Red Hat", "Jobs", and "Events".

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

---

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)