

红帽产品勘误 [RHSA-2025:22035 - Security Advisory](#)

RHSA-2025:22035 - Security Advisory

发布：2025-11-25 已更新：2025-11-25

[概述](#)[更新的软件包](#)

概述

Important: expat security update

类型/严重性

Security Advisory: Important

Red Hat Lightspeed patch analysis

识别并修复受此公告影响的系统。

[查看受影响的系统](#) [↗](#)

标题

An update for expat is now available for Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions.

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.

描述

Expat is a C library for parsing XML documents.

Security Fix(es):

- expat: internal entity expansion (CVE-2013-0340)
- expat: parsing large tokens can trigger a denial of service (CVE-2023-52425)
- 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.

解决方案





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

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




受影响的产品


- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x

修复

- [BZ - 1000109](#)  - CVE-2013-0340 expat: internal entity expansion
- [BZ - 2262877](#)  - CVE-2023-52425 expat: parsing large tokens can trigger a denial of service
- [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

CVE

- [CVE-2013-0340](#) 
- [CVE-2023-52425](#) 
- [CVE-2024-8176](#) 

- [CVE-2025-59375](#) 

参考

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

Red Hat 安全团队联络方式为 secalert@redhat.com。更多联络细节请参考 <https://access.redhat.com/security/team/contact/>。



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

 All systems operational



The image shows a dark-themed footer menu. It starts with a small hat icon. Below it is a list of links: "About Red Hat", "Jobs", "Events", "Locations", "Contact Red Hat", "Red Hat Blog", and "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 and Opt-Out Rights](#)