RHSA-2025:22871 - Security Advisory

Issued: 2025-12-08 Updated: 2025-12-08

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 8.2 Advanced 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):

- expat: internal entity expansion (CVE-2013-0340)
- expat: large number of colons in input makes parser consume high amount of resources, leading to DoS (CVE-2018-20843)
- expat: heap-based buffer over-read via crafted XML input (CVE-2019-15903)
- expat: Large number of prefixed XML attributes on a single tag can crash libexpat (CVE-2021-45960)
- expat: Integer overflow in doProlog in xmlparse.c (CVE-2021-46143)
- expat: Integer overflow in addBinding in xmlparse.c (CVE-2022-22822)
- expat: Integer overflow in build_model in xmlparse.c (CVE-2022-22823)
- expat: Integer overflow in defineAttribute in xmlparse.c (CVE-2022-22824)
- expat: Integer overflow in lookup in xmlparse.c (CVE-2022-22825)
- expat: Integer overflow in nextScaffoldPart in xmlparse.c (CVE-2022-22826)
- expat: Integer overflow in storeAtts in xmlparse.c (CVE-2022-22827)
- expat: integer overflow in the doProlog function (CVE-2022-23990)
- expat: Stack exhaustion in doctype parsing (CVE-2022-25313)
- expat: Integer overflow in copyString() (CVE-2022-25314)
- expat: use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate (CVE-2022-43680)
- 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.

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 Server - AUS 8.2 x86_64

Fixes

- BZ - 1000109 - CVE-2013-0340 expat: internal entity expansion
- BZ - 1723723 - CVE-2018-20843 expat: large number of colons in input makes parser consume high amount of resources, leading to DoS
- BZ - 1752592 - CVE-2019-15903 expat: heap-based buffer over-read via crafted XML input
- BZ - 2044451 - CVE-2021-45960 expat: Large number of prefixed XML attributes on a single tag can crash libexpat
- BZ - 2044455 - CVE-2021-46143 expat: Integer overflow in doProlog in xmlparse.c
- BZ - 2044457 - CVE-2022-22822 expat: Integer overflow in addBinding in xmlparse.c
- BZ - 2044464 - CVE-2022-22823 expat: Integer overflow in build_model in xmlparse.c
- BZ - 2044467 - CVE-2022-22824 expat: Integer overflow in defineAttribute in xmlparse.c
- BZ - 2044479 - CVE-2022-22825 expat: Integer overflow in lookup in xmlparse.c
- BZ - 2044484 - CVE-2022-22826 expat: Integer overflow in nextScaffoldPart in xmlparse.c
- BZ - 2044488 - CVE-2022-22827 expat: Integer overflow in storeAtts in xmlparse.c
- BZ - 2048356 - CVE-2022-23990 expat: integer overflow in the doProlog function
- BZ - 2056350 - CVE-2022-25313 expat: Stack exhaustion in doctype parsing
- BZ - 2056354 - CVE-2022-25314 expat: Integer overflow in copyString()
- BZ - 2140059 - CVE-2022-43680 expat: use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate
- 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

CVEs

- CVE-2013-0340
- CVE-2018-20843
- CVE-2019-15903
- CVE-2021-45960
- CVE-2021-46143
- CVE-2022-22822
- CVE-2022-22823
- CVE-2022-22824
- CVE-2022-22825
- CVE-2022-22826
- CVE-2022-22827
- CVE-2022-23990
- CVE-2022-25313

- CVE-2022-25314
- CVE-2022-43680
- CVE-2023-52425
- CVE-2024-8176
- CVE-2025-59375

References

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

---

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