Red Hat F

RHSA
Advis

5-07-08

Overview

Updated P

Synop

Importa

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 libxml2 is now available for Red Hat Enterprise Linux 10.

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

The libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fix(es):

- libxml: Heap use after free (UAF) leads to Denial of service (DoS) (CVE-2025-49794)
- libxml: Null pointer dereference leads to Denial of service (DoS) (CVE-2025-49795)
- libxml: Type confusion leads to Denial of service (DoS) (CVE-2025-49796)
- libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2 (CVE-2025-6021)

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 10 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat CodeReady Linux Builder for x86_64 10 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x

- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 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

CVEs

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

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/.

All systems operational