



红帽产品勘误 RHSA-2025:10698 - Security Advisory

RHSA-2025:10698 - Security Advisory

发布： 2025-07-09 已更新： 2025-07-09

概述

更新的软件包

概述

Important: libxml2 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 libxml2 is now available for Red Hat Enterprise Linux 8.

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

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: 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.

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 for x86_64 8 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

修复

- [BZ - 2372373](#) - CVE-2025-49794 libxml: Heap use after free (UAF) 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
- [RHEL-74345](#) - "oscap xccdf eval" fails with exit code 1 after printing "No bytes exported: xmlCode: -<randomvalue?>."

CVE



- [CVE-2025-6021](#)


- [CVE-2025-49794](#) 
- [CVE-2025-49796](#) 

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/>。




Quick Links 

Help 

Site Info 

Related Sites 

 Loading



About Red Hat

Jobs

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](#)