CVE

VEX
Public o
Last mo

Jump to section

Description

A use-after-free vulnerability was found in libxml2. This issue occurs when parsing XPath elements under certain circumstances when the XML schematron has the <sch:name path="..."/> schema elements. This flaw allows a malicious actor to craft a malicious XML document used as input for libxml, resulting in the program's crash using libxml or other possible undefined behaviors.

Statement

This issue was rated with a severity impact of Important by Red Hat Product Security, as l ibxml can be used to parse XML coming from the network depending on how the progra m consumes it and uses the library. Additionally, although the initial report shows a crash due to invalid memory access (A:H), other undefined issues that can present data integrit y due to the application overwriting sensitive data are not discarded (I:H).

Mitigation

There's no available mitigation other than avoid processing untrusted XML documents before updating to the libxml version containing the fix.

Additional information

- Bugzilla 2372373: libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- CWE-825: Expired Pointer Dereference

External references

- https://www.cve.org/CVERecord?id=CVE-2025-49794
- https://nvd.nist.gov/vuln/detail/CVE-2025-49794
- https://gitlab.gnome.org/GNOME/libxml2/-/issues/931

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	libxml2
State	Fixed
Justification	None
Errata	RHSA-2025:10630
Release Date	July 8, 2025

Products / Services	Red Hat Enterprise Linux 7 Extended Lifecycle Support
Components	libxml2
State	Fixed
Justification	None
Errata	RHSA-2025:12240
Release Date	July 30, 2025

Products / Services	Red Hat Enterprise Linux 8
Components	libxml2
State	Fixed
Justification	None
Errata	RHSA-2025:10698

1 of 5

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	9.1	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	None	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	None	N/A	N/A
Integrity Impact	High	N/A	N/A
Availability Impact	High	N/A	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Frequently Asked Questions

- **Why is Red Hat's CVSS v3 score or Impact different from other vendors?**
- **My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?**
- **What can I do if my product is listed as "Will not fix"?**
- **What can I do if my product is listed as "Fix deferred"?**
- **What is a mitigation?**
- **I have a Red Hat product but it is not in the above list, is it affected?**
- **Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?**
- **My product is listed as "Out of Support Scope". What does this mean?**

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: March 20, 2026 at 7:11:17 PM UTC