



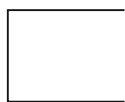
CVE



VEX [↗](#)

Public or

Last mod



Jump to section

Description	Statement	Mitigation	Additional information	Affected Packages	CVSS Score Details	Weakness (CWE)	Acknowledgements	FAQ
-------------	-----------	------------	------------------------	-------------------	--------------------	----------------	------------------	-----

## Description

A flaw was found in libxml2, an XML parsing library. This uncontrolled recursion vulnerability occurs in the xmlCatalogXMLResolveURI function when an XML catalog contains a delegate URI entry that references itself. A remote attacker could exploit this configuration-dependent issue by providing a specially crafted XML catalog, leading to infinite recursion and call stack exhaustion. This ultimately results in a segmentation fault, causing a Denial of Service (DoS) by crashing affected applications.

## Statement

This vulnerability is rated Moderate for Red Hat products. The flaw in libxml2, an XML parsing library, is configuration-dependent and occurs when processing specially crafted XML catalogs with self-referencing delegate URI entries. Exploitation requires an attacker to provide such a cat

alog, leading to a Denial of Service by crashing affected applications.

## Mitigation

Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

## Additional information

- Bugzilla 2429959: libxml2: libxml2: Denial of Service via uncontrolled recursion in XML catalog processing
- CWE-674: Uncontrolled Recursion

### External references

- <https://www.cve.org/CVERecord?id=CVE-2026-0990>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-0990>
- <https://gitlab.gnome.org/GNOME/libxml2/-/issues/1018>

## 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	Fix deferred
Justification	None
Errata	
Release Date	

---

Products / Services	Red Hat Enterprise Linux 6
Components	libxml2
State	Fix deferred
Justification	None
Errata	
Release Date	

---

Products / Services	Red Hat Enterprise Linux 7
Components	libxml2
State	Fix deferred
Justification	None
Errata	

« < 1 of 1 > »

## 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).

 The following CVSS metrics and score provided are preliminary and subject to review.

## CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
<b>CVSS v3 Base Score</b>	5.9	N/A	N/A
<b>Attack Vector</b>	Network	N/A	N/A
<b>Attack Complexity</b>	High	N/A	N/A
<b>Privileges Required</b>	None	N/A	N/A
<b>User Interaction</b>	None	N/A	N/A
<b>Scope</b>	Unchanged	N/A	N/A
<b>Confidentiality Impact</b>	None	N/A	N/A
<b>Integrity Impact</b>	None	N/A	N/A
<b>Availability Impact</b>	High	N/A	N/A

## CVSS v3 Vector

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

## Acknowledgements

Red Hat would like to thank Nick Wellnhofer for reporting this issue.

## 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?	▼

**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: April 9, 2026 at 6:01:16 PM UTC

CVE description copyright © 2021



Quick Links



Help




Site Info



Related Sites



 Partial system outage



[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 and Do Not Sell or Share My Personal Information](#)