CVE-2026-0992

VEX

Public on January 15, 2026

Last modified: April 22, 2026 at 9:30:55 AM UTC

LOW

Low severity

What does this mean?

2.9

CVSS v3 Score Breakdown

Jump to section

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

Description

A flaw was found in the libxml2 library. This uncontrolled resource consumption vulnerability occurs when processing XML catalogs that contain repeated elements pointing to the same downstream catalog. A remote attacker can exploit this by supplying crafted catalogs, causing the parser to redundantly traverse catalog chains. This leads to excessive CPU consumption and degrades application availability, resulting in a denial-of-service condition.

Statement

This vulnerability is rated Low for Red Hat. It affects applications that use the libxml2 library to p rocess XML catalogs. An attacker must locally supply specially crafted XML catalogs containing repeated elements, which can lead to excessive CPU consumption and a denial-of-service cond ition due to redundant catalog chain traversal.

Mitigation

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

Additional information

- Bugzilla 2429975: libxml2: libxml2: Denial of Service via crafted XML catalogs
- CWE-400: Uncontrolled Resource Consumption

External references

- https://www.cve.org/CVERecord?id=CVE-2026-0992
- https://nvd.nist.gov/vuln/detail/CVE-2026-0992
- https://gitlab.gnome.org/GNOME/libxml2/-/issues/1019

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 Hardened Images
Components	libxml2-main
State	Fixed
Justification	None
Errata	RHSA-2026:7519
Release Date	April 10, 2026

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	

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).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	2.9	N/A	N/A
Attack Vector	Local	N/A	N/A
Attack Complexity	High	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	None	N/A	N/A
Availability Impact	Low	N/A	N/A

CVSS v3 Vector

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

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 22, 2026 at 9:30:55 AM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

Service under maintenance