



CVE

VEX [↗](#)

Public or

Last mod



Description

Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Descr

A flaw w

and input

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy settings, then we recognize that you allow an attacker to crash the application or corrupt memory. In some cases, it may lead to denial of service or unexpected behavior.

Statement

This type confusion vulnerability in libxslt has been rated as Important due to its potential to corrupt memory and crash applications during XML transformations. The flaw stems from unsafe reuse of the psvi field between stylesheet and input nodes, causing the program to misinterpret internal data types. When malicious XSLT stylesheets are processed, this confusion can lead to m

emory corruption or denial-of-service. Given libxslt's widespread use in web browsers, server-side applications, and XML processing pipelines, the impact of this vulnerability can extend to user-facing services and backend systems alike.

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 2379228: libxslt: Type confusion in xmlNode.psvi between stylesheet and source nodes
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

External references

- <https://www.cve.org/CVERecord?id=CVE-2025-7424>
- <https://nvd.nist.gov/vuln/detail/CVE-2025-7424>
- <https://gitlab.gnome.org/GNOME/libxslt/-/issues/139>

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	RHBA-2025:12345
Release Date	July 31, 2025

Products / Services	Red Hat Enterprise Linux 10
Components	libxslt
State	Fixed
Justification	None
Errata	RHBA-2025:12345
Release Date	July 31, 2025

Products / Services	Red Hat Enterprise Linux 6
Components	libxslt
State	Out of support scope
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	7.5	7.5	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	Low	Low	N/A
Privileges Required	None	None	N/A
User Interaction	None	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	None	None	N/A
Integrity Impact	None	None	N/A
Availability Impact	High	High	N/A

CVSS v3 Vector

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

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

Understanding the Weakness (CWE)

CWE-843

Availability,Integrity,Confidentiality


Technical Impact:Read Memory; Modify Memory; Execute Unauthorized Code or Commands;
DoS: Crash, Exit, or Restart


When a memory buffer is accessed using the wrong type, it could read or write memory out of the bounds of the buffer, if the allocated buffer is smaller than the type that the code is attempting to access, leading to a crash and possibly code execution.

Acknowledgements

Red Hat would like to thank Ivan Fratric (Google Project Zero) 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? ▼

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: April 14, 2026 at 9:37:15 PM UTC
CVE description copyright © 2021



The image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items, each with a downward arrow: "Quick Links", "Help", "Site Info", and "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 Opt-Out Rights](#)