CVE-2025-7425

VEX

Public on July 10, 2025

Last modified: September 26, 2025 at 8:24:42 AM UTC

IMPORTANT

Important severity

What does this mean?

7.8

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 libxslt where the attribute type, atype, flags are modified in a way that corrupts internal memory management. When XSLT functions, such as the key() process, result in tree fragments, this corruption prevents the proper cleanup of ID attributes. As a result, the system may access freed memory, causing crashes or enabling attackers to trigger heap corruption.

Statement

This heap-use-after-free vulnerability in libxslt is rated Important because it can lead to memor y corruption and application crashes. The flaw arises when internal attribute metadata (atype) is modified by libxslt's xsltSetSourceNodeFlags() function during processing of result tree fragme nts. If the flag corruption prevents proper removal of ID references, later memory cleanup routin

es may operate on already-freed memory. Since libxslt is commonly used in server-side XML pr ocessing, this could result in denial-of-service or potentially facilitate code execution under cert ain memory reuse conditions.

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 2379274: libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr
- CWE-416: Use After Free

External references

- https://www.cve.org/CVERecord?id=CVE-2025-7425
- https://nvd.nist.gov/vuln/detail/CVE-2025-7425
- https://gitlab.gnome.org/GNOME/libxslt/-/issues/140

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 7 Extended Lifecycle Support
Components	libxml2
State	Fixed
Justification	None
Errata	RHSA-2025:13464
Release Date	August 7, 2025

Products / Services	Red Hat Enterprise Linux 8
Components	libxml2
State	Fixed
Justification	None
Errata	RHSA-2025:12450
Release Date	July 31, 2025

Products / Services	Red Hat Enterprise Linux 8.2 Advanced Update Support
Components	libxml2
State	Fixed
Justification	None
Errata	RHSA-2025:13308

1 of 6

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	7.8	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	Changed	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:L/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H

Acknowledgements

Red Hat would like to thank Sergei Glazunov (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: September 26, 2025 at 8:24:42 AM UTC