



Bug 2379274 (CVE-2025-7425) - CVE-2025-7425 libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr

Keywords: Security

Reported: 2025-07-10 09:47 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-23 23:01 UTC ([History](#))

Alias: CVE-2025-7425

CC List: 2 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

- Depends On:** [2379277](#) [2379278](#) [2379279](#)
[2379280](#) [2379284](#) [2379285](#)
[2379286](#) [2379281](#) [2379282](#)
[2379283](#)

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments	(Terms of Use)


Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2025:12528	0	None	None	None	2025-08-04 01:48:35 UTC
Red Hat Product Errata	RHBA-2025:12689	0	None	None	None	2025-08-04 10:31:05 UTC

Red Hat Product Errata	RHBA-2025:12740	0	None	None	None	2025-08-04 14:22:22 UTC
Red Hat Product Errata	RHBA-2025:12741	0	None	None	None	2025-08-04 14:22:20 UTC
Red Hat Product Errata	RHBA-2025:12969	0	None	None	None	2025-08-05 10:36:19 UTC
Red Hat Product Errata	RHBA-2025:12970	0	None	None	None	2025-08-05 10:33:13 UTC
Red Hat Product Errata	RHBA-2025:12971	0	None	None	None	2025-08-05 10:31:22 UTC
Red Hat Product Errata	RHBA-2025:12972	0	None	None	None	2025-08-05 10:37:11 UTC
Red Hat Product Errata	RHBA-2025:13004	0	None	None	None	2025-08-05 12:39:01 UTC
Red Hat Product Errata	RHBA-2025:13008	0	None	None	None	2025-08-05 15:54:30 UTC
Red Hat Product Errata	RHBA-2025:13031	0	None	None	None	2025-08-05 15:47:17 UTC
Red Hat Product Errata	RHBA-2025:13167	0	None	None	None	2025-08-06 09:11:50 UTC
Red Hat Product Errata	RHBA-2025:13248	0	None	None	None	2025-08-06 16:25:11 UTC
Red Hat Product Errata	RHBA-2025:13407	0	None	None	None	2025-08-07 11:08:27 UTC
Red Hat Product Errata	RHBA-2025:13424	0	None	None	None	2025-08-07 14:38:01 UTC
Red Hat	RHBA-2025:13483	0	None	None	None	2025-08-07

Product Errata						17:40:25 UTC
Red Hat Product Errata	RHBA-2025:14637	0	None	None	None	2025-08-26 15:03:16 UTC
Red Hat Product Errata	RHBA-2025:15609	0	None	None	None	2025-09-10 10:43:18 UTC
Red Hat Product Errata	RHSA-2025:12447	0	None	None	None	2025-07-31 15:56:09 UTC
Red Hat Product Errata	RHSA-2025:12450	0	None	None	None	2025-07-31 16:20:58 UTC
Red Hat Product Errata	RHSA-2025:13308	0	None	None	None	2025-08-07 04:42:43 UTC
Red Hat Product Errata	RHSA-2025:13309	0	None	None	None	2025-08-07 04:40:26 UTC
Red Hat Product Errata	RHSA-2025:13310	0	None	None	None	2025-08-07 04:44:04 UTC
Red Hat Product Errata	RHSA-2025:13311	0	None	None	None	2025-08-07 05:18:15 UTC
Red Hat Product Errata	RHSA-2025:13312	0	None	None	None	2025-08-07 05:23:19 UTC
Red Hat Product Errata	RHSA-2025:13313	0	None	None	None	2025-08-07 05:19:09 UTC
Red Hat Product Errata	RHSA-2025:13314	0	None	None	None	2025-08-07 05:25:26 UTC
Red Hat Product Errata	RHSA-2025:13464	0	None	None	None	2025-08-07 16:00:40 UTC
Red Hat Product Errata	RHSA-2025:14059	0	None	None	None	2025-08-27 21:45:19 UTC

Red Hat Product Errata	RHSA-2025:14396	0	None	None	None	2025-08-27 21:45:59 UTC
Red Hat Product Errata	RHSA-2025:14818	0	None	None	None	2025-09-04 17:01:55 UTC
Red Hat Product Errata	RHSA-2025:14819	0	None	None	None	2025-09-02 19:23:54 UTC
Red Hat Product Errata	RHSA-2025:14853	0	None	None	None	2025-09-04 17:04:25 UTC
Red Hat Product Errata	RHSA-2025:14858	0	None	None	None	2025-09-04 17:04:43 UTC
Red Hat Product Errata	RHSA-2025:15308	0	None	None	None	2025-09-11 12:01:10 UTC
Red Hat Product Errata	RHSA-2025:15672	0	None	None	None	2025-09-18 05:45:14 UTC
Red Hat Product Errata	RHSA-2025:15827	0	None	None	None	2025-09-15 15:13:24 UTC
Red Hat Product Errata	RHSA-2025:15828	0	None	None	None	2025-09-15 15:14:12 UTC
Red Hat Product Errata	RHSA-2026:0934	0	None	None	None	2026-01-21 20:21:56 UTC

OSIDB Bzimport  2025-07-10 09:47:37 UTC[Description](#)

Use-After-Free vulnerability in libxslt caused by unsafe manipulation of the atype field in attribute nodes. The flaw occurs when `xsltSetSourceNodeFlags()` sets extra flag bits on `xmlAttrPtr->atype`, a field later used by `libxml2` to check whether an attribute is an XML ID. This corruption can cause `libxml2` to skip cleanup steps like `xmlRemoveID()` during memory deallocation. As a result, ID table entries may point to freed memory, and later calls to `xmlFreeID()` will dereference these dangling pointers, triggering a use-after-free. This vulnerability is exploitable through crafted XSLT using the `key()` function and result tree fragments, and may result in

denial-of-service or memory corruption.

errata-xmlrpc 2025-07-31 15:56:08 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2025:12447 <https://access.redhat.com/errata/RHSA-2025:12447>

errata-xmlrpc 2025-07-31 16:20:57 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2025:12450 <https://access.redhat.com/errata/RHSA-2025:12450>

errata-xmlrpc 2025-08-07 04:40:25 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:13309 <https://access.redhat.com/errata/RHSA-2025:13309>

errata-xmlrpc 2025-08-07 04:42:42 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:13308 <https://access.redhat.com/errata/RHSA-2025:13308>

errata-xmlrpc 2025-08-07 04:44:03 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On

Via RHSA-2025:13310 <https://access.redhat.com/errata/RHSA-2025:13310>

errata-xmlrpc 2025-08-07 05:18:14 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2025:13311 <https://access.redhat.com/errata/RHSA-2025:13311>

errata-xmlrpc 2025-08-07 05:19:08 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions
Red Hat Enterprise Linux 8.8 Telecommunications Update Service

Via RHSA-2025:13313 <https://access.redhat.com/errata/RHSA-2025:13313>

errata-xmlrpc 2025-08-07 05:23:18 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:13312 <https://access.redhat.com/errata/RHSA-2025:13312>

errata-xmlrpc 2025-08-07 05:25:25 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2025:13314 <https://access.redhat.com/errata/RHSA-2025:13314>

errata-xmllrpc 2025-08-07 16:00:38 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:13464 <https://access.redhat.com/errata/RHSA-2025:13464>

errata-xmllrpc 2025-08-27 21:45:18 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via RHSA-2025:14059 <https://access.redhat.com/errata/RHSA-2025:14059>

errata-xmllrpc 2025-08-27 21:45:58 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2025:14396 <https://access.redhat.com/errata/RHSA-2025:14396>

errata-xmllrpc 2025-09-02 19:23:53 UTC

[Comment 16](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.19

Via RHSA-2025:14819 <https://access.redhat.com/errata/RHSA-2025:14819>

errata-xmlrpc 2025-09-04 17:01:54 UTC

[Comment 25](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.18

Via RHSA-2025:14818 <https://access.redhat.com/errata/RHSA-2025:14818>

errata-xmlrpc 2025-09-04 17:04:24 UTC

[Comment 26](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2025:14853 <https://access.redhat.com/errata/RHSA-2025:14853>

errata-xmlrpc 2025-09-04 17:04:41 UTC

[Comment 27](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2025:14858 <https://access.redhat.com/errata/RHSA-2025:14858>

errata-xmlrpc 2025-09-11 12:01:08 UTC

[Comment 36](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.12

Via RHSA-2025:15308 <https://access.redhat.com/errata/RHSA-2025:15308>

errata-xmlrpc 2025-09-15 15:13:23 UTC

[Comment 37](#)

This issue has been addressed in the following products:

Red Hat Web Terminal 1.12 on RHEL 9

Via RHSA-2025:15827 <https://access.redhat.com/errata/RHSA-2025:15827>

[2025:15827](#)

errata-xmlrpc 2025-09-15 15:14:11 UTC

[Comment 38](#)

This issue has been addressed in the following products:

Red Hat Web Terminal 1.11 on RHEL 9

Via RHSA-2025:15828 <https://access.redhat.com/errata/RHSA-2025:15828>

errata-xmlrpc 2025-09-18 05:45:12 UTC

[Comment 39](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.13

Via RHSA-2025:15672 <https://access.redhat.com/errata/RHSA-2025:15672>

errata-xmlrpc 2026-01-21 20:21:54 UTC

[Comment 47](#)

This issue has been addressed in the following products:

RHOSS-1.36-RHEL-8

Via RHSA-2026:0934 <https://access.redhat.com/errata/RHSA-2026:0934>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

