Bug 2372373 (CVE-2025-49794) - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)

Keywords: Security

Status: NEW

Alias: CVE-2025-49794

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2372374 2372377 2372378 2392627 2392628 2392629 2392632 ~~2372375~~ ~~2372376~~ ~~2392630~~ ~~2392631~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-06-12 00:26 UTC by OSIDB Bzimport

Modified: 2026-04-14 09:46 UTC (History)

CC List: 18 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2025:10777	0	None	None	None	2025-07-10 08:11:03 UTC
Red Hat Product Errata	RHBA-2025:10816	0	None	None	None	2025-07-10 16:32:07 UTC

Red Hat Product Errata	RHBA-2025:10826	0	None	None	None	2025-07-10 21:28:29 UTC
Red Hat Product Errata	RHBA-2025:10831	0	None	None	None	2025-07-14 00:18:05 UTC
Red Hat Product Errata	RHBA-2025:10832	0	None	None	None	2025-07-14 00:18:52 UTC
Red Hat Product Errata	RHBA-2025:10833	0	None	None	None	2025-07-14 00:18:56 UTC
Red Hat Product Errata	RHBA-2025:10872	0	None	None	None	2025-07-14 10:11:55 UTC
Red Hat Product Errata	RHBA-2025:11323	0	None	None	None	2025-07-16 12:51:19 UTC
Red Hat Product Errata	RHBA-2025:11901	0	None	None	None	2025-07-28 11:33:57 UTC
Red Hat Product Errata	RHBA-2025:12096	0	None	None	None	2025-07-29 14:49:53 UTC
Red Hat Product Errata	RHBA-2025:12318	0	None	None	None	2025-07-30 20:06:59 UTC
Red Hat Product Errata	RHBA-2025:12374	0	None	None	None	2025-07-31 11:53:55 UTC
Red Hat Product Errata	RHBA-2025:12375	0	None	None	None	2025-07-31 11:55:00 UTC
Red Hat Product Errata	RHSA-2025:10630	0	None	None	None	2025-07-08 21:09:53 UTC
Red Hat Product Errata	RHSA-2025:10698	0	None	None	None	2025-07-09 11:52:12 UTC
Red Hat	RHSA-2025:10699	0	None	None	None	2025-07-09

Product Errata						11:58:20 UTC
Red Hat Product Errata	RHSA-2025:11386	0	None	None	None	2025-07-17 15:27:01 UTC
Red Hat Product Errata	RHSA-2025:11580	0	None	None	None	2025-07-23 04:57:42 UTC
Red Hat Product Errata	RHSA-2025:12098	0	None	None	None	2025-07-29 13:02:14 UTC
Red Hat Product Errata	RHSA-2025:12099	0	None	None	None	2025-07-29 13:01:03 UTC
Red Hat Product Errata	RHSA-2025:12199	0	None	None	None	2025-07-29 15:57:31 UTC
Red Hat Product Errata	RHSA-2025:12237	0	None	None	None	2025-07-30 05:33:34 UTC
Red Hat Product Errata	RHSA-2025:12239	0	None	None	None	2025-07-30 07:08:39 UTC
Red Hat Product Errata	RHSA-2025:12240	0	None	None	None	2025-07-30 07:10:00 UTC
Red Hat Product Errata	RHSA-2025:12241	0	None	None	None	2025-07-30 07:07:16 UTC
Red Hat Product Errata	RHSA-2025:15397	0	None	None	None	2025-10-21 14:49:20 UTC
Red Hat Product Errata	RHSA-2025:15827	0	None	None	None	2025-09-15 15:13:20 UTC
Red Hat Product Errata	RHSA-2025:15828	0	None	None	None	2025-09-15 15:14:21 UTC
Red Hat Product Errata	RHSA-2025:18217	0	None	None	None	2025-10-22 06:19:30 UTC

Red Hat Product Errata	RHSA-2025:18218	0	None	None	None	2025-10-22 05:08:20 UTC
Red Hat Product Errata	RHSA-2025:18240	0	None	None	None	2025-10-23 17:44:36 UTC
Red Hat Product Errata	RHSA-2025:19020	0	None	None	None	2025-10-27 17:46:32 UTC
Red Hat Product Errata	RHSA-2025:19041	0	None	None	None	2025-10-30 05:40:35 UTC
Red Hat Product Errata	RHSA-2025:19046	0	None	None	None	2025-10-29 09:25:14 UTC
Red Hat Product Errata	RHSA-2025:19894	0	None	None	None	2025-11-13 09:44:44 UTC
Red Hat Product Errata	RHSA-2026:0934	0	None	None	None	2026-01-21 20:21:43 UTC

OSIDB Bzimport 2025-06-12 00:26:13 UTC Description

```
A Heap Use After Free (UAF) vulnerability was discovered in
the Schematron in the libxml2. The issue arises in the
xmlSchematronGetNode function when processing XPath
expressions in Schematron schema elements <sch:name
path="..."/>, where a pointer to freed memory is returned and
then accessed, leading to undefined behavior and potential
crashes.
```

errata-xmlrpc 2025-07-08 21:09:51 UTC Comment 2

```
This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2025:10630 https://access.redhat.com/errata/RHSA-
2025:10630
```

errata-xmlrpc 2025-07-09 11:52:10 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2025:10698 https://access.redhat.com/errata/RHSA-2025:10698

errata-xmlrpc 2025-07-09 11:58:18 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2025:10699 https://access.redhat.com/errata/RHSA-2025:10699

errata-xmlrpc 2025-07-17 15:26:59 UTC Comment 10

This issue has been addressed in the following products:

  RHEL-8 based Middleware Containers

Via RHSA-2025:11386 https://access.redhat.com/errata/RHSA-2025:11386

errata-xmlrpc 2025-07-23 04:57:40 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:11580 https://access.redhat.com/errata/RHSA-2025:11580

errata-xmlrpc 2025-07-29 13:01:01 UTC Comment 13

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:12099 https://access.redhat.com/errata/RHSA-

2025:12099

errata-xmlrpc 2025-07-29 13:02:12 UTC Comment 14

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-2025:12098 https://access.redhat.com/errata/RHSA-2025:12098

errata-xmlrpc 2025-07-29 15:57:30 UTC Comment 15

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2025:12199 https://access.redhat.com/errata/RHSA-2025:12199

errata-xmlrpc 2025-07-30 05:33:32 UTC Comment 16

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:12237 https://access.redhat.com/errata/RHSA-2025:12237

errata-xmlrpc 2025-07-30 07:07:14 UTC Comment 17

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-2025:12241 https://access.redhat.com/errata/RHSA-

2025:12241

errata-xmlrpc 2025-07-30 07:08:37 UTC Comment 18

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-2025:12239 https://access.redhat.com/errata/RHSA-2025:12239

errata-xmlrpc 2025-07-30 07:09:59 UTC Comment 19

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:12240 https://access.redhat.com/errata/RHSA-2025:12240

errata-xmlrpc 2025-09-15 15:13:18 UTC Comment 48

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

errata-xmlrpc 2025-09-15 15:14:19 UTC Comment 49

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 2025-10-21 14:49:18 UTC Comment 60

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.20

Via RHSA-2025:15397 https://access.redhat.com/errata/RHSA-2025:15397

errata-xmlrpc 2025-10-22 05:08:17 UTC Comment 61

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.17

Via RHSA-2025:18218 https://access.redhat.com/errata/RHSA-2025:18218

errata-xmlrpc 2025-10-22 06:19:27 UTC Comment 62

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.19

Via RHSA-2025:18217 https://access.redhat.com/errata/RHSA-2025:18217

errata-xmlrpc 2025-10-23 17:44:33 UTC Comment 63

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.13

Via RHSA-2025:18240 https://access.redhat.com/errata/RHSA-2025:18240

errata-xmlrpc 2025-10-27 17:46:29 UTC Comment 64

This issue has been addressed in the following products:

  Red Hat JBoss Core Services 2.4.62.SP2

Via RHSA-2025:19020 https://access.redhat.com/errata/RHSA-2025:19020

errata-xmlrpc 2025-10-29 09:25:12 UTC Comment 65

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.18

Via RHSA-2025:19046 https://access.redhat.com/errata/RHSA-2025:19046

errata-xmlrpc 2025-10-30 05:40:32 UTC Comment 66

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.14

Via RHSA-2025:19041 https://access.redhat.com/errata/RHSA-2025:19041

errata-xmlrpc 2025-11-13 09:44:42 UTC Comment 67

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.12

Via RHSA-2025:19894 https://access.redhat.com/errata/RHSA-2025:19894

errata-xmlrpc 2026-01-21 20:21:40 UTC Comment 68

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.