



Bug 2372406 (CVE-2025-6021) - CVE-2025-6021 libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2

Keywords: Security

Reported: 2025-06-12 07:58 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-03-24 11:24 UTC ([History](#))

Alias: CVE-2025-6021

CC List: 22 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2372411](#) [2372412](#) [2372413](#)
[2372414](#) [2372419](#) [2372420](#)
[2372421](#) [2372422](#) [2372415](#)
[2372416](#) [2372417](#) [2372418](#)

Blocks:

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

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 16:32:06 UTC

Red Hat Product Errata	RHBA-2025:10826	0	None	None	None	2025-07-10 21:28:28 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 00:18:54 UTC
Red Hat Product Errata	RHBA-2025:10833	0	None	None	None	2025-07-14 00:18:58 UTC
Red Hat Product Errata	RHBA-2025:10872	0	None	None	None	2025-07-14 10:11:54 UTC
Red Hat Product Errata	RHBA-2025:11323	0	None	None	None	2025-07-16 12:51:18 UTC
Red Hat Product Errata	RHBA-2025:11901	0	None	None	None	2025-07-28 11:33:59 UTC
Red Hat Product Errata	RHBA-2025:12096	0	None	None	None	2025-07-29 14:49:56 UTC
Red Hat Product Errata	RHBA-2025:12318	0	None	None	None	2025-07-30 20:07:00 UTC
Red Hat Product Errata	RHBA-2025:12374	0	None	None	None	2025-07-31 11:53:58 UTC
Red Hat Product Errata	RHBA-2025:12375	0	None	None	None	2025-07-31 11:54:57 UTC
Red Hat Product Errata	RHSA-2025:10630	0	None	None	None	2025-07-08 21:09:58 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						11:58:21 UTC
Red Hat Product Errata	RHSA-2025:11386	0	None	None	None	2025-07-17 15:27:06 UTC
Red Hat Product Errata	RHSA-2025:11580	0	None	None	None	2025-07-23 04:57:44 UTC
Red Hat Product Errata	RHSA-2025:11673	0	None	None	None	2025-07-29 07:05:25 UTC
Red Hat Product Errata	RHSA-2025:12098	0	None	None	None	2025-07-29 13:02:20 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 15:57:35 UTC
Red Hat Product Errata	RHSA-2025:12237	0	None	None	None	2025-07-30 05:33:40 UTC
Red Hat Product Errata	RHSA-2025:12239	0	None	None	None	2025-07-30 07:08:32 UTC
Red Hat Product Errata	RHSA-2025:12240	0	None	None	None	2025-07-30 07:10:23 UTC
Red Hat Product Errata	RHSA-2025:12241	0	None	None	None	2025-07-30 07:07:11 UTC
Red Hat Product Errata	RHSA-2025:13289	0	None	None	None	2025-08-14 04:08:19 UTC
Red Hat Product Errata	RHSA-2025:13325	0	None	None	None	2025-08-13 05:49:45 UTC
Red Hat Product Errata	RHSA-2025:13336	0	None	None	None	2025-08-13 05:40:35 UTC

Red Hat Product Errata	RHSA-2025:14059	0	None	None	None	2025-08-27 21:45:15 UTC
Red Hat Product Errata	RHSA-2025:14396	0	None	None	None	2025-08-27 21:45:53 UTC
Red Hat Product Errata	RHSA-2025:15308	0	None	None	None	2025-09-11 12:01:06 UTC
Red Hat Product Errata	RHSA-2025:15672	0	None	None	None	2025-09-18 05:45:09 UTC
Red Hat Product Errata	RHSA-2025:19020	0	None	None	None	2025-10-27 17:46:35 UTC

OSIDB Bzimport  2025-06-12 07:58:27 UTC[Description](#)

Integer Overflow (Wraparound) vulnerability in the xmlBuildQName() function in libxml2. The flaw arises due to unsafe arithmetic when concatenating XML name components using the lengths of prefix and local name. These lengths, originally size_t, are cast to int, leading to incorrect calculations when values are large. If exploited, the function can perform a memcpy with an extremely large size, causing a stack buffer overflow. This vulnerability is remotely exploitable if the attacker can influence XML content passed to affected applications, potentially resulting in denial of service.

errata-xmlrpc 2025-07-08 21:09:56 UTC

[Comment 1](#)

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 2](#)

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 11:58:19 UTC

[Comment 3](#)

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 15:27:04 UTC

[Comment 9](#)

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 04:57:41 UTC

[Comment 10](#)

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 07:05:23 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.19

Via RHSA-2025:11673 <https://access.redhat.com/errata/RHSA-2025:11673>

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-xmllrpc 2025-07-29 13:02:17 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-xmllrpc 2025-07-29 15:57:32 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-xmllrpc 2025-07-30 05:33:37 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-xmllrpc 2025-07-30 07:07:09 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 07:08:30 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 07:10:19 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 2025-08-13 05:40:33 UTC

[Comment 33](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2025:13336 <https://access.redhat.com/errata/RHSA-2025:13336>

errata-xmlrpc 2025-08-13 05:49:43 UTC

[Comment 34](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.18

Via RHSA-2025:13325 <https://access.redhat.com/errata/RHSA-2025:13325>

[2025:13325](#)

errata-xmlrpc 2025-08-14 04:08:16 UTC

[Comment 35](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2025:13289 <https://access.redhat.com/errata/RHSA-2025:13289>

errata-xmlrpc 2025-08-27 21:45:12 UTC

[Comment 45](#)

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-xmlrpc 2025-08-27 21:45:51 UTC

[Comment 46](#)

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-xmlrpc 2025-09-11 12:01:04 UTC

[Comment 50](#)

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 2025-09-18 05:45:06 UTC

[Comment 51](#)

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 2025-10-27 17:46:33 UTC

[Comment 62](#)

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>

Note

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

