



# Bug 2423624 (CVE-2025-14905) - CVE-2025-14905 389-ds-base: 389-ds-base: Remote Code Execution and Denial of Service via heap buffer overflow

**Keywords:** Security

**Reported:** 2025-12-18 18:08 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-03-31 00:26 UTC ([History](#))

**Alias:** CVE-2025-14905

**CC List:** 11 users ([show](#))

**Deadline:** 2026-02-20

**Fixed In Version:**

**Product:** Security Response

**Clone Of:**

**Component:** vulnerability

**Environment:**

**Last Closed:**

**Embargoed:**

**Version:** unspecified

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [2450264](#)

**Blocks:**

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


## Attachments [\(Terms of Use\)](#)

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2026:3189</a>	0	None	None	None	2026-02-24 11:35:29 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:3208</a>	0	None	None	None	2026-02-24 13:46:48 UTC
Red Hat	<a href="#">RHSA-2026:3504</a>	0	None	None	None	2026-03-02

Product Errata						06:27:16 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:4207</a>	0	None	None	None	2026-03-10 22:00:31 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:4661</a>	0	None	None	None	2026-03-17 00:15:29 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:4720</a>	0	None	None	None	2026-03-17 10:39:45 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5196</a>	0	None	None	None	2026-03-23 00:17:05 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5511</a>	0	None	None	None	2026-03-24 00:30:23 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5512</a>	0	None	None	None	2026-03-24 00:15:05 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5513</a>	0	None	None	None	2026-03-24 00:47:02 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5514</a>	0	None	None	None	2026-03-24 00:15:40 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5568</a>	0	None	None	None	2026-03-24 08:46:09 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5569</a>	0	None	None	None	2026-03-24 08:47:01 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5576</a>	0	None	None	None	2026-03-24 09:45:46 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5597</a>	0	None	None	None	2026-03-24 10:00:08 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5598</a>	0	None	None	None	2026-03-24 10:13:19 UTC

Red Hat Product Errata	<a href="#">RHSA-2026:6220</a>	0	None	None	None	2026-03-31 00:26:04 UTC
------------------------	--------------------------------	---	------	------	------	-------------------------

OSIDB Bzimport  2025-12-18 18:08:15 UTC[Description](#)

A vulnerability was found in the ds-389-base server, specifically in the schema.c file which was then verified as exploitable in the running server. There is a heap buffer overflow that can be exploited to execute a DoS and potential RCE. The vulnerability is possible through the function `schema_attr_enum_callback`, the code calculates size by summing the lengths of alias strings but fails to account for the formatting characters added during printing. It relies on a static "magic number" of 256 to absorb this overhead. When the number of aliases is large enough, the cumulative overhead of 3 bytes per alias exceeds the 256-byte margin, leading to a heap overflow.

errata-xmlrpc 2026-02-24 11:35:27 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via [RHSA-2026:3189](#) <https://access.redhat.com/errata/RHSA-2026:3189>

errata-xmlrpc 2026-02-24 13:46:46 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via [RHSA-2026:3208](#) <https://access.redhat.com/errata/RHSA-2026:3208>

errata-xmlrpc 2026-03-02 06:27:15 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10.0 Extended Update Support

Via [RHSA-2026:3504](#) <https://access.redhat.com/errata/RHSA-2026:3504>

errata-xmlrpc 2026-03-10 22:00:30 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:4207 <https://access.redhat.com/errata/RHSA-2026:4207>

errata-xmlrpc 2026-03-17 00:15:27 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Directory Server 12.4 EUS for RHEL 9

Via RHSA-2026:4661 <https://access.redhat.com/errata/RHSA-2026:4661>

errata-xmlrpc 2026-03-17 10:39:43 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:4720 <https://access.redhat.com/errata/RHSA-2026:4720>

errata-xmlrpc 2026-03-23 00:17:03 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2026:5196 <https://access.redhat.com/errata/RHSA-2026:5196>

errata-xmlrpc 2026-03-24 00:15:03 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Directory Server 11.5 E4S for RHEL 8

Via RHSA-2026:5512 <https://access.redhat.com/errata/RHSA-2026:5512>

[2026:5512](#)

errata-xmlrpc 2026-03-24 00:15:38 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Directory Server 11.9 for RHEL 8

Via RHSA-2026:5514 <https://access.redhat.com/errata/RHSA-2026:5514>

errata-xmlrpc 2026-03-24 00:30:22 UTC

[Comment 12](#)

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-2026:5511 <https://access.redhat.com/errata/RHSA-2026:5511>

errata-xmlrpc 2026-03-24 00:47:01 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:5513 <https://access.redhat.com/errata/RHSA-2026:5513>

errata-xmlrpc 2026-03-24 08:46:07 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat Directory Server 11.7 E4S for RHEL 8

Via RHSA-2026:5568 <https://access.redhat.com/errata/RHSA-2026:5568>

errata-xmlrpc 2026-03-24 08:46:59 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Directory Server 12.2 E4S for RHEL 9

Via RHSA-2026:5569 <https://access.redhat.com/errata/RHSA-2026:5569>

errata-xmlrpc 2026-03-24 09:45:44 UTC

[Comment 16](#)

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-2026:5576 <https://access.redhat.com/errata/RHSA-2026:5576>

errata-xmlrpc 2026-03-24 10:00:06 UTC

[Comment 17](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2026:5597 <https://access.redhat.com/errata/RHSA-2026:5597>

errata-xmlrpc 2026-03-24 10:13:18 UTC

[Comment 18](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2026:5598 <https://access.redhat.com/errata/RHSA-2026:5598>

errata-xmlrpc 2026-03-31 00:26:02 UTC

[Comment 19](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2026:6220 <https://access.redhat.com/errata/RHSA-2026:6220>

---

Note

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

