



Bug 2413081 (CVE-2025-12801) - CVE-2025-12801 nfs-utils: rpc.mountd in the nfs-utils privilege escalation [NEEDINFO]

Keywords: ✕ ▼

Status: NEW

Alias: CVE-2025-12801

Deadline: 2026-03-04

Product: Security Response

Component: vulnerability

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:

Blocks:

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

Reported: 2025-11-06 12:19 UTC by OSIDB Bzimport

Modified: 2026-04-01 09:16 UTC ([History](#))

CC List: 6 users ([show](#))

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:


Flags: carnil: needinfo? (prodsec-dev)

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:3938	0	None	None	None	2026-03-05 18:53:22 UTC
Red Hat Product Errata	RHSA-2026:3939	0	None	None	None	2026-03-05 18:40:17 UTC
Red Hat	RHSA-2026:3940	0	None	None	None	2026-03-05

Product Errata						18:54:49 UTC
Red Hat Product Errata	RHSA-2026:3941	0	None	None	None	2026-03-05 19:08:41 UTC
Red Hat Product Errata	RHSA-2026:3942	0	None	None	None	2026-03-05 19:04:34 UTC
Red Hat Product Errata	RHSA-2026:5127	0	None	None	None	2026-03-25 04:58:03 UTC
Red Hat Product Errata	RHSA-2026:5867	0	None	None	None	2026-04-01 09:16:50 UTC

OSIDB Bzimport  2025-11-06 12:19:04 UTC[Description](#)

A vulnerability was recently discovered in the rpc.mountd daemon in the nfs-utils package for Linux, that allows a NFSv3 client to escalate the privileges assigned to it in the /etc/exports file at mount time. In particular, it allows the client to access any subdirectory or subtree of an exported directory, regardless of the set file permissions, and regardless of any 'root_squash' or 'all_squash' attributes that would normally be expected to apply to that client.

errata-xmlrpc 2026-03-05 18:40:16 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via [RHSA-2026:3939](#) <https://access.redhat.com/errata/RHSA-2026:3939>

errata-xmlrpc 2026-03-05 18:53:21 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via [RHSA-2026:3938](#) <https://access.redhat.com/errata/RHSA-2026:3938>

2026:3938

errata-xmlrpc 2026-03-05 18:54:48 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:3940 <https://access.redhat.com/errata/RHSA-2026:3940>

errata-xmlrpc 2026-03-05 19:04:32 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:3942 <https://access.redhat.com/errata/RHSA-2026:3942>

errata-xmlrpc 2026-03-05 19:08:40 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:3941 <https://access.redhat.com/errata/RHSA-2026:3941>

Salvatore Bonaccorso 2026-03-06 06:43:54 UTC

[Comment 7](#)

Hi

Can you please provide references to the upstream commit fixing this issue?

Regards,
Salvatore

Salvatore Bonaccorso 2026-03-06 19:46:22 UTC

[Comment 11](#)

There was this linux-nfs post: <https://lore.kernel.org/linux-nfs/20260305155948.11261-1-steved@redhat.com/>

errata-xmlrpc 2026-03-25 04:58:01 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.18

Via RHSA-2026:5127 <https://access.redhat.com/errata/RHSA-2026:5127>

errata-xmlrpc 2026-04-01 09:16:48 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via RHSA-2026:5867 <https://access.redhat.com/errata/RHSA-2026:5867>

Note

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

