CVE-2025-12801

VEX

Public on March 4, 2026

Last modified: March 5, 2026 at 7:05:54 PM UTC

MODERATE

Moderate severity

What does this mean?

6.5

CVSS v3 Score Breakdown

Insights vulnerability analysis

View exposed systems →

Jump to section

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.

Statement

This MODERATE impact vulnerability in `rpc.mountd` within the `nfs-utils` package allows an authenticated NFSv3 client to bypass configured `root_squash` or `all_squash` restrictions. This enables the client to access subdirectories of an exported NFS share with elevated privileges, regardless of the intended file permissions. Red Hat Enterprise Linux systems configured as NFSv3 servers are affected.

Mitigation

Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Additional information

- Bugzilla 2413081: nfs-utils: rpc.mountd in the nfs-utils privilege escalation
- CWE-279: Incorrect Execution-Assigned Permissions

External references

- https://www.cve.org/CVERecord?id=CVE-2025-12801
- https://nvd.nist.gov/vuln/detail/CVE-2025-12801

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	nfs-utils
State	Fixed
Justification	None
Errata	RHSA-2026:3939
Release Date	March 6, 2026

Products / Services	Red Hat Enterprise Linux 8
Components	nfs-utils
State	Fixed
Justification	None
Errata	RHSA-2026:3938
Release Date	March 5, 2026

Products / Services	Red Hat Enterprise Linux 9
Components	nfs-utils
State	Fixed
Justification	None
Errata	RHSA-2026:3940

1 of 2

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	6.5	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	Low	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	High	N/A	N/A
Integrity Impact	None	N/A	N/A
Availability Impact	None	N/A	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Understanding the Weakness (CWE)

CWE-279

Confidentiality,Integrity

Technical Impact:Read Application Data; Modify Application Data

Acknowledgements

Red Hat would like to thank Simon Hall for reporting this issue.

Frequently Asked Questions

- **Why is Red Hat's CVSS v3 score or Impact different from other vendors?**
- **My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?**
- **What can I do if my product is listed as "Will not fix"?**
- **What can I do if my product is listed as "Fix deferred"?**
- **What is a mitigation?**
- **I have a Red Hat product but it is not in the above list, is it affected?**
- **Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?**
- **My product is listed as "Out of Support Scope". What does this mean?**

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: March 5, 2026 at 7:05:54 PM UTC

Cool Stuff Store

Red Hat Summit
