



# Nfs-utils: rpc.mountd in the nfs-utils privilege escalation

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2025-12801
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-04 16:16:23 UTC
<b>Updated</b>	2026-04-01 11:15:57 UTC
<b>Description</b>	A vulnerability was recently discovered in the rpc.mountd daemon in the nfs-utils package for Linux, that allows a NFSv3 cli

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from secalert@redhat.com

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

**EPSS:** 0.000130000 probability, percentile 0.019430000 (date 2026-04-01)

**Problem Types:** CWE-279 | CWE-732 | CWE-279 Incorrect Execution-Assigned Permissions

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux-nfs	Nfs-utils	-	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 1:2.8.3-0.el10_1.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 1:2.3.3-68.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 1:2.5.4-38.el9_7.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 1:2.5.4-38.el9_7.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 1:2.5.4-26.el9_4.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 1:2.5.4-34.el9_6.3 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.17	unaffected 417.94.202603242359-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.18	unaffected 418.94.202603181125-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.19	unaffected 4.19.9.6.202603251941-0 * rpm
CNA	Red Hat	Red Hat Ceph Storage 8	unaffected sha256:1160569002c25d3d349bbe41b57eeffade4:
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified

### References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:5606	secalert@redhat.com	<a href="https://access.redhat.com/errata/RHSA-2026:5606">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2026:5867	secalert@redhat.com	<a href="https://access.redhat.com/errata/RHSA-2026:5867">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2026:5127	secalert@redhat.com	<a href="https://access.redhat.com/errata/RHSA-2026:5127">access.redhat.com</a>	

<a href="https://access.redhat.com/errata/RHSA-2026:3942">access.redhat.com/errata/RHSA-2026:3942</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://access.redhat.com/errata/RHSA-2026:3941">access.redhat.com/errata/RHSA-2026:3941</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://access.redhat.com/errata/RHSA-2026:3939">access.redhat.com/errata/RHSA-2026:3939</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://access.redhat.com/errata/RHSA-2026:5877">access.redhat.com/errata/RHSA-2026:5877</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2026:3940">access.redhat.com/errata/RHSA-2026:3940</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://access.redhat.com/errata/RHSA-2026:3938">access.redhat.com/errata/RHSA-2026:3938</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking, Third Party Advisory
<a href="https://access.redhat.com/security/cve/CVE-2025-12801">access.redhat.com/security/cve/CVE-2025-12801</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Red Hat would like to thank Simon Hall for reporting this issue. (en)

### Additional Advisory Data

Source	Time	Event
CNA	2025-11-06T12:15:57.744Z	Reported to Red Hat.
CNA	2026-03-04T15:06:00.000Z	Made public.

#### Workarounds

**CNA:** 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.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)