



# hv\_netvsc: Fix panic during namespace deletion with VF

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

## Summary

<b>CVE</b>	CVE-2025-38683
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-04 16:15:36 UTC
<b>Updated</b>	2026-05-12 13:16:54 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: hv\_netvsc: Fix panic during namespace deletion with VF 1

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-476

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 3eb6aa870057da9f1304db660f68b9c2eb7e856d 3ca41ab55d23a0aa71661a5a56a8f06c1
CNA	Linux	Linux	affected b7a396f76ada277d049558db648389456458af65 3467c4ebb334658c6fcf3eabb64a6e8b2
CNA	Linux	Linux	affected 4faa6e3e66b3251eb4bf5761d2f3f0f14095aaca 4eff1e57a8ef98d70451b94e8437e458b27c
CNA	Linux	Linux	affected 62c85b9a0dd7471a362170323e1211ad98ff7b4b 2a70cbd1aef8b8be39992ab7b776ce139
CNA	Linux	Linux	affected 4c262801ea60c518b5bebc22a09f5b78b3147da2 d036104947176d030bec64792d54e1b4
CNA	Linux	Linux	affected 4c262801ea60c518b5bebc22a09f5b78b3147da2 5276896e6923ebe8c68573779d784aaf7
CNA	Linux	Linux	affected 4c262801ea60c518b5bebc22a09f5b78b3147da2 4293f6c5ccf735b26afeb6825def14d830c
CNA	Linux	Linux	affected 4c262801ea60c518b5bebc22a09f5b78b3147da2 33caa208dba6fa639e8a92fd0c8320b65
CNA	Linux	Linux	affected 7abd221a55a61b6b2bf0e80f850bfc0ae75c7e01 git
CNA	Linux	Linux	affected 31a38a908c98aebc7a1104dab5f1ba199f234b7b git
CNA	Linux	Linux	affected 04d748d4bd2d86739b159563f257e3dc5492c88d git
CNA	Linux	Linux	affected 6.12
CNA	Linux	Linux	unaffected 6.12 semver
CNA	Linux	Linux	unaffected 5.10.241 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.190 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.43 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.11 6.15.* semver
CNA	Linux	Linux	unaffected 6.16.2 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

## References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/2a70cbd1aef8b8be39992ab7b776ce1390091774	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d036104947176d030bec64792d54e1b4f4c7f318	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/5276896e6923ebe8c68573779d784aaf7d987cce	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/3467c4ebb334658c6fcf3eabb64a6e8b2135e010	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/4293f6c5ccf735b26afeb6825def14d830e0367b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/3ca41ab55d23a0aa71661a5a56a8f06c11db90dc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.co</a>
git.kernel.org/stable/c/4eff1e57a8ef98d70451b94e8437e458b27dd234	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/33caa208dba6fa639e8a92fd0c8320b652e5550c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

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