



# iommu/vt-d: Skip dev-iotlb flush for inaccessible PCIe device without scalable mode

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

## Summary

<b>CVE</b>	CVE-2026-43161
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:34 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Skip dev-iotlb flush for inaccessible PCIe dev

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 37764b952e1b39053defc7ebe5dcd8c4e3e78de9 48b3f08e68b29a79527869cdde7298ca2a9b9646 g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 37764b952e1b39053defc7ebe5dcd8c4e3e78de9 e70d5feb10c5ba2bbf7ca400b8f39a2f82d653e8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 37764b952e1b39053defc7ebe5dcd8c4e3e78de9 bc0490ad9edf5c6f98e39fbbee2877b85261a5ae git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 37764b952e1b39053defc7ebe5dcd8c4e3e78de9 42662d19839f34735b718129ea200e3734b07e50 g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 99301a53a1378f8863ac7850b9589f997bb0e125 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 948ec6d003280d49aca49b366aa5cb140f87434d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.14
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.14 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.77 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.17 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.6 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/42662d19839f34735b718129ea200e3734b07e50	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/e70d5feb10c5ba2bbf7ca400b8f39a2f82d653e8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/48b3f08e68b29a79527869cdde7298ca2a9b9646	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/bc0490ad9edf5c6f98e39fbbee2877b85261a5ae	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

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

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