



iommu/vt-d: Flush dev-IOTLB only when PCIe device is accessible in scalable mode

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

Summary

CVE	CVE-2026-43130
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:30 UTC
Updated	2026-05-06 13:07:51 UTC

Description In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Flush dev-IOTLB only when PCIe device is accessible in scalable mode

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected f873b85ec762c5a6abe94a7ddb31df5d3ba07d85 581ce094d9eafb78ec4f9de77bd24b780c151236 git
CNA	Linux	Linux	affected d70f1c85113cd8c2aa8373f491ca5d1b22ec0554 e2c78c69f8faf2885ea4ceee08c71ac738f401a0 git
CNA	Linux	Linux	affected 34a7b30f56d30114bf4d436e4dc793afe326fbcf ead67d0378e90f419e385a43af29435242d80c12 git
CNA	Linux	Linux	affected 2b74b2a92e524d7c8dec8e02e95ecf18b667c062 01aed2f1d7cb8dfd4c60c5bb4727608cb82b401d git
CNA	Linux	Linux	affected 4fc82cd907ac075648789cc3a00877778aa1838b 9813306610d0d718c863aaa70928bf57d7570ec0 git
CNA	Linux	Linux	affected 4fc82cd907ac075648789cc3a00877778aa1838b 9deaacc8dcaddb6ddc5b52e1e63b457450ec0f94 git
CNA	Linux	Linux	affected 4fc82cd907ac075648789cc3a00877778aa1838b 0da6697e577023d8867c7beb2d16a22510e4eea9 git
CNA	Linux	Linux	affected 4fc82cd907ac075648789cc3a00877778aa1838b 10e60d87813989e20eac1f3eda30b3bae461e7f9 git
CNA	Linux	Linux	affected c04f2780919f20e2cc4846764221f5e802555868 git
CNA	Linux	Linux	affected 025bc6b41e020aeb1e71f84ae3ffce945026de05 git
CNA	Linux	Linux	affected 6.9
CNA	Linux	Linux	unaffected 6.9 semver
CNA	Linux	Linux	unaffected 5.10.252 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ead67d0378e90f419e385a43af29435242d80c12	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/581ce094d9eafb78ec4f9de77bd24b780c151236	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/01aed2f1d7cb8fdf4c60c5bb4727608cb82b401d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/10e60d87813989e20eac1f3eda30b3bae461e7f9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e2c78c69f8faf2885ea4ceee08c71ac738f401a0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0da6697e577023d8867c7beb2d16a22510e4eea9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9deaacc8dcaddb6ddc5b52e1e63b457450ec0f94	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9813306610d0d718c863aaa70928bf57d7570ec0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

© 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). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report