



PCI: hv: Fix double ida_free in hv_pci_probe error path

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

Summary

CVE	CVE-2026-43097
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 10:16:23 UTC
Updated	2026-05-06 10:16:23 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: PCI: hv: Fix double ida_free in hv_pci_probe error path If I

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected bcce8c74f1ce1e2731ac0261287897e3768767d8 21bc8e0ba5c2a081b0a2808c976d4c9dbddf1e48 git
CNA	Linux	Linux	affected bcce8c74f1ce1e2731ac0261287897e3768767d8 b6422dff0e518245019233432b6bccfc30b73e2f git
CNA	Linux	Linux	affected 6.19
CNA	Linux	Linux	unaffected 6.19 semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/b6422dff0e518245019233432b6bccfc30b73e2f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/21bc8e0ba5c2a081b0a2808c976d4c9dbddf1e48	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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