



PCI: endpoint: Fix swapped parameters in pci_{primary/secondary}_epc_epf_unlink() functions

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

Summary

CVE	CVE-2026-43200
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:39 UTC
Updated	2026-05-11 20:10:53 UTC

Description In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: Fix swapped parameters in pci_{primary/se

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: NVD-CWE-noinfo

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 e85a2d7837622bd99c96f5bbc7f972da90c285a2 58686bf62cb38b92e4b28408162a5703775b4d12 gi
CNA	Linux	Linux	affected e85a2d7837622bd99c96f5bbc7f972da90c285a2 1c96c1acef4b4a1108fc13f84a8ac0b0633bbb46 git
CNA	Linux	Linux	affected e85a2d7837622bd99c96f5bbc7f972da90c285a2 142b1bba3299264b76ed8ef53cd93b2b2af65d6c git
CNA	Linux	Linux	affected e85a2d7837622bd99c96f5bbc7f972da90c285a2 339191811e6fc4559c4008c5af7a91b05086d596 git
CNA	Linux	Linux	affected e85a2d7837622bd99c96f5bbc7f972da90c285a2 733cbc3aa97e71cc70847e75c925b364cc9b04a6 gi
CNA	Linux	Linux	affected e85a2d7837622bd99c96f5bbc7f972da90c285a2 aefc0e0bd20f54abe3b501b8798c0be656af272b git
CNA	Linux	Linux	affected e85a2d7837622bd99c96f5bbc7f972da90c285a2 8754dd7639ab0fd68c3ab9d91c7bdecc3e5740a8 git
CNA	Linux	Linux	affected 5.12
CNA	Linux	Linux	unaffected 5.12 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
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/58686bf62cb38b92e4b28408162a5703775b4d12	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/733cbc3aa97e71cc70847e75c925b364cc9b04a6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/1c96c1acef4b4a1108fc13f84a8ac0b0633bbb46	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/142b1bba3299264b76ed8ef53cd93b2b2af65d6c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/339191811e6fc4559c4008c5af7a91b05086d596	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/aefc0e0bd20f54abe3b501b8798c0be656af272b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8754dd7639ab0fd68c3ab9d91c7bdecc3e5740a8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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](#) 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](#)