



# net: ipa: fix event ring index not programmed for IPA v5.0+

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

## Summary

<b>CVE</b>	CVE-2026-43345
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 14:16:44 UTC
<b>Updated</b>	2026-05-11 08:16:10 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net: ipa: fix event ring index not programmed for IPA v5.0-

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

**EPSS:** 0.000180000 probability, percentile 0.049330000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected faf0678ec8a0aa9039d8b188d012206abd67dd5c ae8343a19ccb051d519dbb3a9082ddea9f0551d3 gi
CNA	Linux	Linux	affected faf0678ec8a0aa9039d8b188d012206abd67dd5c 2bf18b643c4656413f7cfd5615af60a6b4e261da git
CNA	Linux	Linux	affected faf0678ec8a0aa9039d8b188d012206abd67dd5c 2d2dc166d55148cfcf8ae67b415f8d6d110e6fca git
CNA	Linux	Linux	affected faf0678ec8a0aa9039d8b188d012206abd67dd5c 34c988bb04cbdf093d2134e179433da49ffcd044 git
CNA	Linux	Linux	affected faf0678ec8a0aa9039d8b188d012206abd67dd5c 56007972c0b1e783ca714d6f1f4d6e66e531d21f git
CNA	Linux	Linux	affected 6.4
CNA	Linux	Linux	unaffected 6.4 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* 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/2d2dc166d55148cfcf8ae67b415f8d6d110e6fca	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/34c988bb04cbdf093d2134e179433da49ffcd044	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/56007972c0b1e783ca714d6f1f4d6e66e531d21f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/2bf18b643c4656413f7cfd5615af60a6b4e261da	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/ae8343a19ccb051d519dbb3a9082ddea9f0551d3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://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.

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](https://cve.report/api)

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