



# net: dsa: microchip: Fix error path in PTP IRQ setup

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

## Summary

<b>CVE</b>	CVE-2026-43372
<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 15:16:48 UTC
<b>Updated</b>	2026-05-12 14:10:27 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: net: dsa: microchip: Fix error path in PTP IRQ setup If req

## Risk And Classification

**EPSS:** 0.000180000 probability, percentile 0.049210000 (date 2026-05-11)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3b5a6115d6ea45df1ea65dc9b832b23db5d593ba3704ac6a0d9a78f66a187515a8ca3faedaf01cc5 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1ba6da6ca3db76f6a39004fd33a9c990e428515e e80fef36c676c947072dabeb5803ae59d92ba493 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d0b8fec8ae50525b57139393d0bb1f446e82ff7e 6c58a9fdb0d0e1011aa02455d26d6ebeam251979b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d0b8fec8ae50525b57139393d0bb1f446e82ff7e c2d1d41e0e8ec447d40a5752844fc5fb0b23db27 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d0b8fec8ae50525b57139393d0bb1f446e82ff7e 99c8c16a4aad0b37293cae213e15957c573cf79b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ae12e4e0ca231475bcef841c6a6722fa185fd520 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.18
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.19 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.9 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/c2d1d41e0e8ec447d40a5752844fc5fb0b23db27	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

git.kernel.org/stable/c/3704ac6a0d9a78f66a187515a8ca3faedaf01cc5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/6c58a9fdb0d0e1011aa02455d26d6ebea251979b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/e80fef36c676c947072dabeb5803ae59d92ba493	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/99c8c16a4aad0b37293cae213e15957c573cf79b	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.

© [CVE.report](https://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/cve). 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)