



# clk: mediatek: fix of \_iomap memory leak

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

## Summary

<b>CVE</b>	CVE-2023-53424
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-18 16:15:46 UTC
<b>Updated</b>	2026-04-06 14:01:05 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: clk: mediatek: fix of _iomap memory leak Smatch reports: c

## 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:** CWE-401 | CWE-401 CWE-401 Missing Release of Memory after Effective Lifetime

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

## 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 c58cd0e40ffac67961b945793876b973728f9b80 847d5dd788ce05f0aaaa36ea174f7f0b9cf86f7d git
CNA	Linux	Linux	affected c58cd0e40ffac67961b945793876b973728f9b80 2cae6a28d8c12c597e8656962271520434c61c48 git
CNA	Linux	Linux	affected c58cd0e40ffac67961b945793876b973728f9b80 47234e19b00816a8a7b278c7173f6d4e928c43c7 git
CNA	Linux	Linux	affected c58cd0e40ffac67961b945793876b973728f9b80 3db7285e044144fd88a356f5b641b9cd4b231a77 git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.164 6.1.* semver
CNA	Linux	Linux	unaffected 6.3.13 6.3.* semver
CNA	Linux	Linux	unaffected 6.4.4 6.4.* semver
CNA	Linux	Linux	unaffected 6.5 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/2cae6a28d8c12c597e8656962271520434c61c48	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/3db7285e044144fd88a356f5b641b9cd4b231a77	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/847d5dd788ce05f0aaaa36ea174f7f0b9cf86f7d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/47234e19b00816a8a7b278c7173f6d4e928c43c7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
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](#) 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](#)