



# crypto: omap - Allocate OMAP\_CRYPTO\_FORCE\_COPY scatterlists correctly

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

## Summary

<b>CVE</b>	CVE-2026-23222
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-18 16:22:31 UTC
<b>Updated</b>	2026-04-02 15:16:23 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: crypto: omap - Allocate OMAP\_CRYPTO\_FORCE\_COPY

## 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

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	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 953c81941b0ad373674656b8767c00234ebf17ac g
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 31aff96a41ae6f1f1687c065607875a27c364da8 git
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 79f95b51d4278044013672c27519ae88d07013d8 g
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 6edf8df4bd29f7bfd245b67b2c31d905f1cfc14b git
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 c184341920ed78b6466360ed7b45b8922586c38f g
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 2ed27b5a1174351148c3adbfc0cd86d54072ba2e g
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 d1836c628cb72734eb5f7dfd4c996a9c18bba3ad git
CNA	Linux	Linux	affected 74ed87e7e7f7197137164738dd0610ccd5ec5ed1 1562b1fb7e17c1b3addb15e125c718b2be7f5512 gi
CNA	Linux	Linux	affected 4.13
CNA	Linux	Linux	unaffected 4.13 semver
CNA	Linux	Linux	unaffected 5.10.251 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.201 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.164 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.125 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.72 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.11 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.1 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc1 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/c184341920ed78b6466360ed7b45b8922586c38f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/c184341920ed78b6466360ed7b45b8922586c38f">git.kernel.org</a>	Patch
git.kernel.org/stable/c/2ed27b5a1174351148c3adbfc0cd86d54072ba2e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/2ed27b5a1174351148c3adbfc0cd86d54072ba2e">git.kernel.org</a>	Patch
git.kernel.org/stable/c/6edf8df4bd29f7bfd245b67b2c31d905f1cfc14b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/6edf8df4bd29f7bfd245b67b2c31d905f1cfc14b">git.kernel.org</a>	Patch

<a href="https://git.kernel.org/stable/c/79f95b51d4278044013672c27519ae88d07013d8">git.kernel.org/stable/c/79f95b51d4278044013672c27519ae88d07013d8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/31aff96a41ae6f1f1687c065607875a27c364da8">git.kernel.org/stable/c/31aff96a41ae6f1f1687c065607875a27c364da8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/d1836c628cb72734eb5f7dfd4c996a9c18bba3ad">git.kernel.org/stable/c/d1836c628cb72734eb5f7dfd4c996a9c18bba3ad</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/953c81941b0ad373674656b8767c00234ebf17ac">git.kernel.org/stable/c/953c81941b0ad373674656b8767c00234ebf17ac</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/1562b1fb7e17c1b3addb15e125c718b2be7f5512">git.kernel.org/stable/c/1562b1fb7e17c1b3addb15e125c718b2be7f5512</a>	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](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](https://www.mitre.org/cve).

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