



media: verisilicon: AV1: Fix tile info buffer size

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-43222
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:41 UTC
Updated	2026-05-08 21:12:57 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: media: verisilicon: AV1: Fix tile info buffer size Each tile in

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000130000 probability, percentile 0.023990000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
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

High

Integrity

High

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 727a400686a2c0d25015c9e44916a59b72882f83 a5b1ddbe31f49b4da78642157589970e9b60a231 c
CNA	Linux	Linux	affected 727a400686a2c0d25015c9e44916a59b72882f83 34f36f9c6114af781a5a4f7a7c99334c85b73fc7 git
CNA	Linux	Linux	affected 727a400686a2c0d25015c9e44916a59b72882f83 f122f2b3ce9dbde60bf7ab0b180fe4a01f9d9bc4 git
CNA	Linux	Linux	affected 727a400686a2c0d25015c9e44916a59b72882f83 74abfadd7ef5ac9f3a6111d550cc651d1457c641 git
CNA	Linux	Linux	affected 727a400686a2c0d25015c9e44916a59b72882f83 a505ca2db89ad92a8d8d27fa68ebafb12e04a679 gi
CNA	Linux	Linux	affected 6.5
CNA	Linux	Linux	unaffected 6.5 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/a5b1ddbe31f49b4da78642157589970e9b60a231	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/a505ca2db89ad92a8d8d27fa68ebafb12e04a679	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/74abfadd7ef5ac9f3a6111d550cc651d1457c641	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f122f2b3ce9dbde60bf7ab0b180fe4a01f9d9bc4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/34f36f9c6114af781a5a4f7a7c99334c85b73fc7	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](#)