



# drm/i915/dsi: Don't do DSC horizontal timing adjustments in command mode

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

## Summary

<b>CVE</b>	CVE-2026-31767
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-01 15:16:39 UTC
<b>Updated</b>	2026-05-11 17:53:02 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: drm/i915/dsi: Don't do DSC horizontal timing adjustments

## 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

**EPSS:** 0.000180000 probability, percentile 0.046430000 (date 2026-05-05)

**Problem Types:** CWE-369

## 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 53693f02d80e0a909e76c2a25f8aac8515f959db 55efe8402f46af8399c8b634a18b130a05fd7820 git
CNA	Linux	Linux	affected 53693f02d80e0a909e76c2a25f8aac8515f959db 86e926b108880c0109b8635e459450447156aeb7 gi
CNA	Linux	Linux	affected 53693f02d80e0a909e76c2a25f8aac8515f959db 33b5336e4fd8ba0e40a12989cadb3f5534a0f9e4 git
CNA	Linux	Linux	affected 53693f02d80e0a909e76c2a25f8aac8515f959db 4dfce79e098915d8e5fc2b9e1d980bc3251dd32c git
CNA	Linux	Linux	affected 5.6
CNA	Linux	Linux	unaffected 5.6 semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/33b5336e4fd8ba0e40a12989cadb3f5534a0f9e4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/55efe8402f46af8399c8b634a18b130a05fd7820	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/4dfce79e098915d8e5fc2b9e1d980bc3251dd32c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/86e926b108880c0109b8635e459450447156aeb7	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.

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)