



# USB: dummy-hcd: Fix locking/synchronization error

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-43327
<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 14:16:42 UTC
<b>Updated</b>	2026-05-15 18:05:56 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: USB: dummy-hcd: Fix locking/synchronization error Syzbc

## 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:** 0.000240000 probability, percentile 0.070360000 (date 2026-05-12)

**Problem Types:** CWE-667

## 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 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 6350c7dd33ab481ef41c931a238361490c32d15c git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 cc97fb5969177cccce2e23b31298df220fc7570d git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 218886b2ef2dea7627d3700ab0abaf4bf9d1161f git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 791966f85b439b261bf19865cf1c07c065ffb4b4 git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 805b1833d6ed6da5086e610578a28e71bb54fbbb git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 efb9441f1e769a7aae1813d497cec09cbdf031 git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 69ab97a693251d6a6093e630060a3c744fd58524 git
CNA	Linux	Linux	affected 7dbd8f4cabd96db5a50513de9d83a8105a5ffc81 616a63ff495df12863692ab3f9f7b84e3fa7a66d git
CNA	Linux	Linux	affected 7b416b9dac6ede26d4ca0c1a88b448b543623ff3 git
CNA	Linux	Linux	affected 8590bc1da625dd4a589eac0fc3aa3cf4f400424d git
CNA	Linux	Linux	affected a867d5b932ac4911d3f8a1e63505061b0c81f889 git
CNA	Linux	Linux	affected e84b4a008365b7edbd842a063ae28d040a98db25 git
CNA	Linux	Linux	affected e39b17143a5b5aac81f066d455e5d3a9877eb3ae git
CNA	Linux	Linux	affected 4f8ae1fcb0dfbb72a7678f81bf01fb7fc85c6715 git
CNA	Linux	Linux	affected 4.14
CNA	Linux	Linux	unaffected 4.14 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* 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/efbd9441f1e769a7aae1813d497cec09cbdf031	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/6350c7dd33ab481ef41c931a238361490c32d15c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch

<a href="https://git.kernel.org/stable/c/616a63ff495df12863692ab3f9f7b84e3fa7a66d">git.kernel.org/stable/c/616a63ff495df12863692ab3f9f7b84e3fa7a66d</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/cc97fb5969177cccce2e23b31298df220fc7570d">git.kernel.org/stable/c/cc97fb5969177cccce2e23b31298df220fc7570d</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/218886b2ef2dea7627d3700ab0abaf4bf9d1161f">git.kernel.org/stable/c/218886b2ef2dea7627d3700ab0abaf4bf9d1161f</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/69ab97a693251d6a6093e630060a3c744fd58524">git.kernel.org/stable/c/69ab97a693251d6a6093e630060a3c744fd58524</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/791966f85b439b261bf19865cf1c07c065ffb4b4">git.kernel.org/stable/c/791966f85b439b261bf19865cf1c07c065ffb4b4</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/805b1833d6ed6da5086e610578a28e71bb54fbbb">git.kernel.org/stable/c/805b1833d6ed6da5086e610578a28e71bb54fbbb</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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

**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)