



udp: Fix wildcard bind conflict check when using hash2

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

Summary

CVE	CVE-2026-31503
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:48 UTC
Updated	2026-04-22 14:16:48 UTC

Description In the Linux kernel, the following vulnerability has been resolved: udp: Fix wildcard bind conflict check when using hash2 W

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 30fff9231fad757c061285e347b33c5149c2c2e4 d6ace0dbcbb7fd285738bb87b42b71b01858c952 git
CNA	Linux	Linux	affected 30fff9231fad757c061285e347b33c5149c2c2e4 2297e38114316b26ae02f2d205c49b5511c5ed55 git
CNA	Linux	Linux	affected 30fff9231fad757c061285e347b33c5149c2c2e4 f1bed05a832ae79be5f7a105da56810eaa59a5f1 git
CNA	Linux	Linux	affected 30fff9231fad757c061285e347b33c5149c2c2e4 18d84c45def3671d5c89fbd5d4ab8a3217fe4b4 git
CNA	Linux	Linux	affected 30fff9231fad757c061285e347b33c5149c2c2e4 0a360f7f73a06ac88f18917055fbcc79694252d7 git
CNA	Linux	Linux	affected 30fff9231fad757c061285e347b33c5149c2c2e4 e537dd15d0d4ad989d56a1021290f0c674dd8b28 git
CNA	Linux	Linux	affected 2.6.33
CNA	Linux	Linux	unaffected 2.6.33 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.131 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/18d84c45def3671d5c89fbd5d4ab8a3217fe4b4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2297e38114316b26ae02f2d205c49b5511c5ed55	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d6ace0dbcbb7fd285738bb87b42b71b01858c952	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

git.kernel.org/stable/c/0a360f7f73a06ac88f18917055fbcc79694252d7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/e537dd15d0d4ad989d56a1021290f0c674dd8b28	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f1bed05a832ae79be5f7a105da56810eaa59a5f1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
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](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/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report