



# udp\_tunnel: fix NULL deref caused by udp\_sock\_create6 when CONFIG\_IPV6=n

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

## Summary

<b>CVE</b>	CVE-2026-23439
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-03 16:16:25 UTC
<b>Updated</b>	2026-04-18 09:16:26 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: udp\_tunnel: fix NULL deref caused by udp\_sock\_create6

## Risk And Classification

**EPSS:** 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 dfc96ae0074cc47b5478a59e5aa19233e434243f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 66117dbb3dbae82f86735bf727b1d59cc677afa1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 ba7c9ddcdd077942b798979edb035207374d4096 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 a05a2149386f6dfb4245f522acdbef892acafc84 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 9f036aa0fe46c19e938f03d10e02c23f4ffae5e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 003343985f26dfefd0c94b1fe1316a2de74428b9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 12aa4b73a67d95bc739995a2d6943aec2f9785c9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fd384412e199b62c3ddaabd18dce86d0e164c5b9 b3a6df291fecf5f8a308953b65ca72b7fc9e015d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.18
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.18 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.20 6.18.* semver

CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.10 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/b3a6df291fecf5f8a308953b65ca72b7fc9e015d">git.kernel.org/stable/c/b3a6df291fecf5f8a308953b65ca72b7fc9e015d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/dfc96ae0074cc47b5478a59e5aa19233e434243f">git.kernel.org/stable/c/dfc96ae0074cc47b5478a59e5aa19233e434243f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9f036aa0fe46c19e938f03d10e02c23f4fffae5e">git.kernel.org/stable/c/9f036aa0fe46c19e938f03d10e02c23f4fffae5e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ba7c9ddcdd077942b798979edb035207374d4096">git.kernel.org/stable/c/ba7c9ddcdd077942b798979edb035207374d4096</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/003343985f26dfefd0c94b1fe1316a2de74428b9">git.kernel.org/stable/c/003343985f26dfefd0c94b1fe1316a2de74428b9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/12aa4b73a67d95bc739995a2d6943aec2f9785c9">git.kernel.org/stable/c/12aa4b73a67d95bc739995a2d6943aec2f9785c9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a05a2149386f6dfb4245f522acdbef892acafc84">git.kernel.org/stable/c/a05a2149386f6dfb4245f522acdbef892acafc84</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/66117dbb3dbae82f86735bf727b1d59cc677afa1">git.kernel.org/stable/c/66117dbb3dbae82f86735bf727b1d59cc677afa1</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
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](#) 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](https://cve.report/api)

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