



vxlan: validate ND option lengths in vxlan_na_create

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

Summary

CVE	CVE-2026-31738
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:36 UTC
Updated	2026-05-07 18:58:07 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: vxlan: validate ND option lengths in vxlan_na_create vxlan

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 0.068060000 (date 2026-05-05)

Problem Types: NVD-CWE-noinfo

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 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa 901c1dd3bab2955d7e664f914c374c8c3ac2b958 git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa e476745917a1e288eb15e7ff49d286a86a4861d3 git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa 2029712fb2c87e9a8c75094906f2ee29bf08c500 git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa 602596c69a70e50d9ab8c6ae0290a01f88229dd7 git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa de20d2e3b9179d132f5f5b44e490d7c916c6321b git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa eddfce70a6f3107d1679b0c2fcb96b593bd679 git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa b69c4236255bd8de16cd876e58c6f0867d1d78b1 git
CNA	Linux	Linux	affected 4b29dba9c085a4fb79058fb1c45a2f6257ca3dfa afa9a05e6c4971bd5586f1b304e14d61fb3d9385 git
CNA	Linux	Linux	affected d8be18c52dbc94989f6d74637b731af39cd3d902 git
CNA	Linux	Linux	affected 3927dace523706cc00f808520eaf2125dd7c07b5 git
CNA	Linux	Linux	affected 3.14
CNA	Linux	Linux	unaffected 3.14 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/eddfce70a6f3107d1679b0c2fcb96b593bd679	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/e476745917a1e288eb15e7ff49d286a86a4861d3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2029712fb2c87e9a8c75094906f2ee29bf08c500	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b69c4236255bd8de16cd876e58c6f0867d1d78b1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/de20d2e3b9179d132f5f5b44e490d7c916c6321b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/602596c69a70e50d9ab8c6ae0290a01f88229dd7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch

git.kernel.org/stable/c/afa9a05e6c4971bd5586f1b304e14d61fb3d9385	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/901c1dd3bab2955d7e664f914c374c8c3ac2b958	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](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/cve).

Free CVE JSON API cve.report/api

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