



netfilter: nf_tables: fix inverted genmask check in nft_map_catchall_activate()

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

Summary

CVE	CVE-2026-23111
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-13 14:16:10 UTC
Updated	2026-04-03 14:16:23 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix inverted genmask check in nft_map_catchall_activate()

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-416

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 25aa2ad37c2162be1c0bc4fe6397f7e4c13f00f8 8c760ba4e36c750379d13569f23f5a6e185333f5 git
CNA	Linux	Linux	affected d60be2da67d172aecf866302c91ea11533eca4d9 b9b6573421de51829f7ec1cce76d85f5f6fbbd7f git
CNA	Linux	Linux	affected 628bd3e49cba1c066228e23d71a852c23e26da73 42c574c1504aa089a0a142e4c13859327570473d
CNA	Linux	Linux	affected 628bd3e49cba1c066228e23d71a852c23e26da73 1444ff890b4653add12f734ffeffc173d42862dd git
CNA	Linux	Linux	affected 628bd3e49cba1c066228e23d71a852c23e26da73 8b68a45f9722f2babe9e7bad00aa74638addf081 gi
CNA	Linux	Linux	affected 628bd3e49cba1c066228e23d71a852c23e26da73 f41c5d151078c5348271ffaf8e7410d96f2d82f8 git
CNA	Linux	Linux	affected bc9f791d2593f17e39f87c6e2b3a36549a3705b1 git
CNA	Linux	Linux	affected 3c7ec098e3b588434a8b07ea9b5b36f04cef1f50 git
CNA	Linux	Linux	affected a136b7942ad2a50de708f76ea299ccb45ac7a7f9 git
CNA	Linux	Linux	affected dc7cdf8cbcbf8b13de1df93f356ec04cdeef5c41 git
CNA	Linux	Linux	affected 6.4
CNA	Linux	Linux	unaffected 6.4 semver
CNA	Linux	Linux	unaffected 5.15.200 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.163 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.124 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.70 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.10 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/8b68a45f9722f2babe9e7bad00aa74638addf081	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/42c574c1504aa089a0a142e4c13859327570473d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b9b6573421de51829f7ec1cce76d85f5f6fbbd7f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch

git.kernel.org/stable/c/1444ff890b4653add12f734ffeffc173d42862dd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f41c5d151078c5348271ffaf8e7410d96f2d82f8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8c760ba4e36c750379d13569f23f5a6e185333f5	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](#).

Free CVE JSON API cve.report/api

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