



# netfilter: ipset: drop logically empty buckets in mtype\_del

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

## Summary

<b>CVE</b>	CVE-2026-31418
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 14:16:11 UTC
<b>Updated</b>	2026-04-18 09:16:31 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: drop logically empty buckets in mtype\_del

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.066100000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 c098ff857e7ca923539164af5b3c2fe3e8f8afaf git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 58f3a14826d4e6b0d5421f1a64be280b48601ea2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 ad92ee87462f9a3061361d392e9dbfe2e5c1c9fb git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 6cea34d7ec6829b62f521a37a287f670144a2233 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 b7eef00f08b92b0b9efe8ae0df6d0005e6199323 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 68ca0eea0af02bed36c5e2c13e9fa1647c31a7d4 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 ceacaa76f221a6577aba945bb8873c2e640aeba4 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8af1c6fbd9239877998c7f5a591cb2c88d41fb66 9862ef9ab0a116c6dca98842aab7de13a252ae02 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6c717726f341fd8f39a3ec2dcf5d98d9d28a2769 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d2997d64dfa65082236bca1efd596b6c935daf5e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.6
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.6 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 6.1.168 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.134 6.6.* semver

CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.81 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.22 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.12 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/b7eef00f08b92b0b9efe8ae0df6d0005e6199323">git.kernel.org/stable/c/b7eef00f08b92b0b9efe8ae0df6d0005e6199323</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/58f3a14826d4e6b0d5421f1a64be280b48601ea2">git.kernel.org/stable/c/58f3a14826d4e6b0d5421f1a64be280b48601ea2</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/6cea34d7ec6829b62f521a37a287f670144a2233">git.kernel.org/stable/c/6cea34d7ec6829b62f521a37a287f670144a2233</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9862ef9ab0a116c6dca98842aab7de13a252ae02">git.kernel.org/stable/c/9862ef9ab0a116c6dca98842aab7de13a252ae02</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ceacaa76f221a6577aba945bb8873c2e640aeba4">git.kernel.org/stable/c/ceacaa76f221a6577aba945bb8873c2e640aeba4</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/68ca0eea0af02bed36c5e2c13e9fa1647c31a7d4">git.kernel.org/stable/c/68ca0eea0af02bed36c5e2c13e9fa1647c31a7d4</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/c098ff857e7ca923539164af5b3c2fe3e8f8afaf">git.kernel.org/stable/c/c098ff857e7ca923539164af5b3c2fe3e8f8afaf</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ad92ee87462f9a3061361d392e9dbfe2e5c1c9fb">git.kernel.org/stable/c/ad92ee87462f9a3061361d392e9dbfe2e5c1c9fb</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)