



# xfrm: always flush state and policy upon NETDEV\_UNREGISTER event

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

## Summary

<b>CVE</b>	CVE-2026-43167
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:34 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: xfrm: always flush state and policy upon NETDEV\_UNRE

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d77e38e612a017480157fe6d2c1422f42cb5b7e3 166801e49a5b5fc127b8c9e2f110f303cfdffbc3 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d77e38e612a017480157fe6d2c1422f42cb5b7e3 a3c8fede034fa27892f87c863cbd5493167d17ed git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d77e38e612a017480157fe6d2c1422f42cb5b7e3 59581778792cbaf8ad788f4a21dc663ce986050e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d77e38e612a017480157fe6d2c1422f42cb5b7e3 8c75c455ecd3bfd2f36abf66edb7021c4fa19ec4 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected d77e38e612a017480157fe6d2c1422f42cb5b7e3 4efa91a28576054aae0e6dad9cba8fed8293aef8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.12 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.128 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.75 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.16 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.6 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/166801e49a5b5fc127b8c9e2f110f303cfdffbc3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/4efa91a28576054aae0e6dad9cba8fed8293aef8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/8c75c455ecd3bfd2f36abf66edb7021c4fa19ec4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/59581778792cbaf8ad788f4a21dc663ce986050e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

git.kernel.org/stable/c/a3c8fede034fa27892f87c863cbd5493167d17ed	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>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

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](https://cve.report/api)

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