



net/mlx5: Fix switchdev mode rollback in case of failure

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

Summary

CVE	CVE-2026-43012
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:45 UTC
Updated	2026-05-01 15:24:14 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix switchdev mode rollback in case of failure If

Risk And Classification

EPSS: 0.000180000 probability, percentile 0.046430000 (date 2026-05-05)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected de85624c623dbb5fdb3ae7b08b66894a072c0cc0 2ebb13f3e8be0b61f72425b34cce60c8b6ad1891 git
CNA	Linux	Linux	affected 2a4f56bcc473d8faeb29b73082df39efbe5893c e27153b2bd6e6699b544ac4dfa35d167bed5e642 git
CNA	Linux	Linux	affected 2a4f56bcc473d8faeb29b73082df39efbe5893c 4363698838b7ec6e8d85b179495889aa7e522f91 git
CNA	Linux	Linux	affected 2a4f56bcc473d8faeb29b73082df39efbe5893c 403186400a1a6166efe7031edc549c15fee4723f git
CNA	Linux	Linux	affected 6.13
CNA	Linux	Linux	unaffected 6.13 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/4363698838b7ec6e8d85b179495889aa7e522f91	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/403186400a1a6166efe7031edc549c15fee4723f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2ebb13f3e8be0b61f72425b34cce60c8b6ad1891	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e27153b2bd6e6699b544ac4dfa35d167bed5e642	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

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 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

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