



net/mlx5e: RX, Fix XDP multi-buf frag counting for legacy RQ

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

Summary

CVE	CVE-2026-43464
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:59 UTC
Updated	2026-05-11 08:16:15 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: RX, Fix XDP multi-buf frag counting for legacy

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000170000 probability, percentile 0.043040000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected afd5ba577c10639f62e8120df67dc70ea4b61176 c74557495efb4bd0adefdfc8678ecdbc82a06da3 git
CNA	Linux	Linux	affected afd5ba577c10639f62e8120df67dc70ea4b61176 03cb50e5b74fce8bf6d92b860371b66253cf0f8d git
CNA	Linux	Linux	affected afd5ba577c10639f62e8120df67dc70ea4b61176 a6413e6f6c9d9bb9833324cb3753582f7bc0f2fa git
CNA	Linux	Linux	affected 72328f25755ee966724f46e3a0e8e59bef2091ba git
CNA	Linux	Linux	affected 0049fd63881505566824e88cfa624638f921c808 git
CNA	Linux	Linux	affected d969645b9b7810289bf3c353ea06957373756b8e git
CNA	Linux	Linux	affected 6.18
CNA	Linux	Linux	unaffected 6.18 semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/c74557495efb4bd0adefdfc8678ecdbc82a06da3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a6413e6f6c9d9bb9833324cb3753582f7bc0f2fa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/03cb50e5b74fce8bf6d92b860371b66253cf0f8d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web](https://www.mitre.org)

[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