



net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()

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

Summary

CVE	CVE-2024-26882
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-17 11:15:10 UTC
Updated	2026-05-12 12:16:23 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel

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: NVD-CWE-noinfo | CWE-noinfo Not enough information

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	ADP	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

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 c54419321455631079c7d6e60bc732dd0c5914c5 ec6bb
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 77fd5
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 5c033
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 60044
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 c4c85
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 f6723
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 ca914
CNA	Linux	Linux	affected c54419321455631079c7d6e60bc732dd0c5914c5 b0ec2
CNA	Linux	Linux	affected 3.10
CNA	Linux	Linux	unaffected 3.10 semver
CNA	Linux	Linux	unaffected 5.4.273 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.214 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.153 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.83 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.23 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.11 6.7.* semver
CNA	Linux	Linux	unaffected 6.8.2 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org

git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/f6723d8dbfdc10c784a56748f86a9a3cd410dbd5	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/ec6bb01e02cbd47781dd90775b631a1dc4bd9d2b	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
git.kernel.org/stable/c/ca914f1cdee8a85799942c9b0ce5015bbd6844e1	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
security.netapp.com/advisory/ntap-20241220-0002	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com
git.kernel.org/stable/c/c4c857723b37c20651300b3de4ff25059848b4b0	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/b0ec2abf98267f14d032102551581c833b0659d3	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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