



net: Fix icmp host relookup triggering ip_rt_bug

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

Summary

CVE	CVE-2024-56647
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-27 15:15:24 UTC
Updated	2026-05-17 16:16:13 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net: Fix icmp host relookup triggering ip_rt_bug arp link fai

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000090000 probability, percentile 0.008870000 (date 2026-05-17)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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
Operating System	Linux	Linux Kernel	6.13	rc1	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 8b7817f3a959ed99d7443afc12f78a7e1fcc2063 da54b3039d436227deebbc202cefea63bd318a38 git
CNA	Linux	Linux	affected 8b7817f3a959ed99d7443afc12f78a7e1fcc2063 9545011e7b2a8fc0cbd6e387a09f12cd41d7d82f git
CNA	Linux	Linux	affected 8b7817f3a959ed99d7443afc12f78a7e1fcc2063 c44daa7e3c73229f7ac74985acb8c7fb909c4e0a git
CNA	Linux	Linux	affected 2.6.25
CNA	Linux	Linux	unaffected 2.6.25 semver
CNA	Linux	Linux	unaffected 6.6.140 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.5 6.12.* semver
CNA	Linux	Linux	unaffected 6.13 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/da54b3039d436227deebbc202cefea63bd318a38	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c44daa7e3c73229f7ac74985acb8c7fb909c4e0a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9545011e7b2a8fc0cbd6e387a09f12cd41d7d82f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.

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](#)