ipv4: check for NULL idev in ip_route_use_hint()

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-36008
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-20 10:15:14 UTC
Updated	2026-05-12 12:16:47 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv4: check for NULL idev in ip_route_use_hint() syzbot w

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

Problem Types: CWE-476

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 02b24941619fcce3d280311ac73b1e461552
CNA	Linux	Linux	affected 02b24941619fcce3d280311ac73b1e461552
CNA	Linux	Linux	affected 02b24941619fcce3d280311ac73b1e461552
CNA	Linux	Linux	affected 02b24941619fcce3d280311ac73b1e461552
CNA	Linux	Linux	affected 02b24941619fcce3d280311ac73b1e461552
CNA	Linux	Linux	affected 02b24941619fcce3d280311ac73b1e461552
CNA	Linux	Linux	affected 5.5
CNA	Linux	Linux	unaffected 5.5 semver
CNA	Linux	Linux	unaffected 5.10.216 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.158 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.90 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.30 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.9 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/58a4c9b1e5a3e53c9148e80b90e1e43897ce77d1	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/c71ea3534ec0936fc57e6fb271c7cc6a2f68c295	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/8240c7308c941db4d9a0a91b54eca843c616a655	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/7da0f91681c4902bc5c210356fdd963b04d5d1d4	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/7a25bfd12733a8f38f8ca47c581f876c3d481ac0	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/03b5a9b2b526862b21bcc31976e393a6e63785d1	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 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 registred 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**