



# ipv6: avoid possible NULL deref in rt6\_uncached\_list\_flush\_dev()

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

## Summary

<b>CVE</b>	CVE-2024-47707
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-21 12:15:07 UTC
<b>Updated</b>	2026-05-12 12:17:14 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: ipv6: avoid possible NULL deref in rt6\_uncached\_list\_flush

## 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 e332bc67cf5e5e5b71a1aec9750d0791aac65183 a61a1
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 8a8b8
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 e43dd
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 f2bd96
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 0ceb2
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 9a0dd
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 08409
CNA	Linux	Linux	affected e332bc67cf5e5e5b71a1aec9750d0791aac65183 04cce
CNA	Linux	Linux	affected 58d772c203ee57c45620730198bc2d9ded7a1464 git
CNA	Linux	Linux	affected 4.3
CNA	Linux	Linux	unaffected 4.3 semver
CNA	Linux	Linux	unaffected 5.4.290 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.234 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.177 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.113 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.54 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.13 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.2 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom

## References

Reference	Source	Link
cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.c

<a href="https://git.kernel.org/stable/c/9a0ddc73be37d19dff1ba08290af34e707d18e50">git.kernel.org/stable/c/9a0ddc73be37d19dff1ba08290af34e707d18e50</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/03/msg00002.html">lists.debian.org/debian-lts-announce/2025/03/msg00002.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/e43dd28405e6b9935279996725ee11e6306547a5">git.kernel.org/stable/c/e43dd28405e6b9935279996725ee11e6306547a5</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/f2bd9635543ca41533b870f420872819f8331823">git.kernel.org/stable/c/f2bd9635543ca41533b870f420872819f8331823</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/04ccecf959d3b9ae7348780d8e379c6486176ac">git.kernel.org/stable/c/04ccecf959d3b9ae7348780d8e379c6486176ac</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.com/productcert/html/ssa-265688.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="https://git.kernel.org/stable/c/0ceb2f2b5c813f932d6e60d3feec5e7e713da783">git.kernel.org/stable/c/0ceb2f2b5c813f932d6e60d3feec5e7e713da783</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/8a8b83016f06805775db099c8377024b6fa5b975">git.kernel.org/stable/c/8a8b83016f06805775db099c8377024b6fa5b975</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/a61a174280dad99f25a7dee920310885daf2552b">git.kernel.org/stable/c/a61a174280dad99f25a7dee920310885daf2552b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/08409e401622e2896b4313be9f781bde8a2a6a53">git.kernel.org/stable/c/08409e401622e2896b4313be9f781bde8a2a6a53</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/01/msg00001.html">lists.debian.org/debian-lts-announce/2025/01/msg00001.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)