



ipv6: prevent UAF in ip6_send_skb()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2024-44987
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-04 20:15:07 UTC
Updated	2026-05-12 12:17:09 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an L

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: CWE-416

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 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 0625491493d9000e4556bf566d205c28c8e7
CNA	Linux	Linux	affected 2.6.32
CNA	Linux	Linux	unaffected 2.6.32 semver
CNA	Linux	Linux	unaffected 4.19.321 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.283 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.225 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.166 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.107 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.48 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.7 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.2 custom
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.2 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 V3.2 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
git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/cb5880a0de12c7f618d2bdd84e2d985f1e06ed7e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/af1dde074ee2ed7dd5bdca4e7e8ba17f44e7b011	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ce2f6cfab2c637d0bd9762104023a15d0ab7c0a8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/faa389b2fbaaec7fd27a390b4896139f9da662e3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	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/571567e0277008459750f0728f246086b2659429	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/e44bd76dd072756e674f45c5be00153f4ded68b2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
lists.debian.org/debian-lts-announce/2024/10/msg00003.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.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 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